МЕГАТРЕНД УНИВЕРЗИТЕТ БЕОГРАД
ФАКУЛТЕТ ЗА КОМПЈУТЕРСКЕ НАУКЕ

Дејан В. Кожовић

МУЛТИДИСЦИПЛИНАРНИ АСПЕКТИ САЈБЕР БЕЗБЕДНОСТИ АВИО СИСТЕМА ADS–B

докторска дисертација

Београд, 2023

MEGATREND UNIVERSITY BELGRADE
FACULTY OF COMPUTER SCIECE

Dejan V. Kožović

MULTIDISCIPLINARY ASPECTS OF CYBER SECURITY OF ADS-B AVIATION SYSTEM

Doctoral dissertation

Belgrade, 2023

Ментор:

проф. др Немања Мачек

Факултет друштвених наука у Београду, Универзитет Привредна академија у Новом Саду

Чланови комисије:

1. проф. др Драган Ђурђевић, Факултет за цивилно ваздухопловство, Мегатренд Универзитет, Београд, Србија
2. др Емил Бањац, ванр. проф., Факултет за цивилно ваздухопловство, Мегатренд Универзитет, Београд, Србија

Датум одбране:_____

Изјава захвалности

Као што се често дешава, бављење темом отворило је нова питања и интересовања. Осим личног рада и промишљања, омогућило је и остваривање стручне сарадње и стицање нових пријатељстава. Надам се да ће овај рад бити од користи мојим колегама – пилотима, али и свима онима који се на одређени начин сусрећу и баве питањима сајбер безбедности, да ће подстаћи нове идеје и бити путоказ за нека будућа научна истраживања, као и допринети безбедности авијације у целини.

Захваљујем се мом ментору, проф. Немањи Мачеку на саветима, искуству, залагању и свесрдној помоћи коју ми је пружио у изради овог рада. Нарочиту и велику захвалност дугујем проф. Драгану Ђурђевићу на пруженом стручном знању, научно-методолошком приступу, посвећености и подршци, као и људском разумевању.

Хвала мојим пријатељима, Марини и Саши Стаменовић, Ивану Поповићу и Контроли летења СМАТСА, драгим Благојевићима, колегама и пријатељима, професорима Мирку Динуловићу, Бошку Рашуу и Марти Трнинић. Били су подршка и помоћ када је било потребно...

Хвала мојој Наташи, која ме је непрекидно храбрила и подстицала на упорност и истрајност.

Овај рад посвећујем мојим родитељима, мајци Драгани и оцу Владимиру, који су ме увек усмеравали тако да поштујем знање и рад, као и да верујем у победу стрпљења, упорности и доброте.

Аутор

МУЛТИДИСЦИПЛИНАРНИ АСПЕКТИ САЈБЕР БЕЗБЕДНОСТИ АВИО СИСТЕМА ADS–B

Резиме

У време информационих и комуникационих технологија, функционисање авио сектора, заснива се на интер- и интра повезивању компјутерских система, који омогућавају бројне оперативне бенефите. Међутим, ово повезивање утиче на то да инфраструктурни авио-системи постају рањиви на различите врсте сајбер напада коришћењем постојећих хардвера и софтвера, што представља велики безбедносни ризик. Наиме, ваздухопловна телекомуникациона мрежа јесте *ad-hoc* бежична мрежа која има велики број мобилних чворова, а ова мобилност, као најслабија карика у ланцу, може се искористити за предузимање потенцијалног сајбер напада. Тако, један од авио-система који се ослања на технологију сателитског позиционирања је *Automatic Dependent Surveillance – Broadcast* (ADS–B), чије је увођење представљало гигански корак у модернизацији и побољшању квалитета ваздухопловних операција. Ова нова генерација технологије надзора ваздушног саобраћаја, интегрише постојећа техничка решења из области телекомуникација, навигације и осматрања ваздушног простора, како би се пилотима и контролорима летења обезбедиле правовремене информације за доношење одлука. ADS–B функционише у два режима: ADS–B Out (систем који омогућава аутоматско емитовање података, о положају, висини, брзини и другим параметрима, од ваздухоплова до ATC на земљи, тј. функција која се односи на комуникацију између ваздухоплова и ATC) и ADS–B In (опциона услуга, којом адекватно опремљен ваздухоплов, може да прима и прикаже детаљне информације о другим ваздухопловима из окружења, тј. функција која омогућава међусобну комуникацију између ваздухоплова), који пружају бројне бенефите, као што су аутономност и ефикасност летења, уштеда ресурса, заштита животне средине, итд. ADS–B Out постаје обавезан глобални стандард, док ADS–B In остаје опциона функција. Међутим, ADS–B емитује информације преко отворених и нешифрованих протокола, тако да се може лако компромитовати коришћењем постојећих хардвера и софтвера, што представља велики безбедносни ризик. Тако, ADS–B може бити изложен различитим врстама сајбер напада, као што су прислушкивање (*eavesdropping*), ометање (*jamming)* и лажирање (*spoofing*). Као против-мере овим нападима, предложу се различите технике, од криптографских, преко техника које користе верификацију локације, до техника машинског учења (вештачке интелигенције). Поред постојећих сигурносних решења и протокола, *International Civil Aviation Organization* (ICAO) и друге организације, радне групе и конференције, континуирано анализирају и прате ефикасне сајбер против-мере/методе и њихову интеграцију у системе контроле летења, комуникације и навигације. Такође, приступ проблему сајбер безбедности (нарочито ADS–B), осим техничко-организационе базе која представља баријеру, а која спречава да сајбер напад продре до авиона/кокпита, захтева и интеграцију људског фактора (посада авиона/пилот) у сајбер-одбрамбени слој, или, шта више, да пилот буде последња линија одбране – јер, потпуно је јасно да су људске одлуке засноване на претходним знањима и способностима, неопходност за превазилажење/решавање критичних ситуација. Иако је према процени ICAO, ризик од успешног сајбер напада с

губитком људских живота, у односу на друге облике терористичких напада, релативно низак, ипак, најскорије, евидентирани су бројни случајеви нарушавања оперативности авиокомпанија услед различитих сајбер инцидената, који, наизглед малог обима, али с тенденцијом пораста, могу имати много шире и озбиљније последице. У том контексту, циљ ове дисертације је истраживање неких од главних питања сајбер безбедности у авијацији, нарочито ADS–B система, тј. потенцијалним искоришћењем ADS–B рањивости и њихов утицај на ваздухопловне операције, затим, систематска квалитативна и интерпретативна анализа реалних сајбер претњи/инцидената у цивилној авијацији, као и примена ADS–B у анализи најскорије евидентираних инцидентних ситуација у ваздухопловству. Такође, анализа укључује и персонално искуство аутора у области цивилне авијације, што доприноси свеобухватнијем сагледавању проблема.

Кључне речи: ADS–B, GPS/GNSS, цивилна авијација, информационо-комуникационе технологије, безбедност, рањивости, сајбер напад, тероризам

Научна област: мултидисциплинарни, интердисциплинарни, компјутерске науке

Ужа научна област: рачунарске науке

MULTIDISCIPLINARY ASPECTS OF CYBER SECURITY OF ADS-B AVIATION SYSTEMS

Abstract

In the age of information and communication technologies, the functioning of the aviation sector is based on the inter- and intra connection of computer systems, which enable numerous operational benefits in aviation. However, this connectivity has the effect of making infrastructure aviation systems vulnerable to various types of cyber attacks, using existing hardware and software, which poses a major security risk. Namely, the aviation telecommunications network is an ad-hoc wireless network that has a large number of mobile nodes, and this mobility, as the weakest link in the chain, can be used to undertake a potential cyber attack. Thus, one of the aviation systems that relies on satellite positioning technology is Automatic Dependent Surveillance – Broadcast (ADS–B), the introduction of which represented a giant step in the modernization and improvement of the quality of aviation operations. This new generation of air traffic control technology integrates existing technical solutions in the fields of telecommunications, navigation and airspace surveillance to provide pilots and air traffic controllers with timely information for decision-making. ADS–B works in two modes: ADS–B Out (a system that enables the automatic transmission of data on the position, altitude, speed and other parameters of the aircraft, from the aircraft to the ATC on the ground, i.e. the function related to the communication between the aircraft and the ATC) and ADS–B In (an optional service, with which an adequately equipped aircraft can receive and display detailed information about other aircraft in the environment, i.e. a function that enables mutual communication between aircraft), which provides numerous benefits, such as autonomy and flight efficiency, resource saving, environmental protection, etc. ADS–B Out becomes a mandatory global standard, while ADS–B In remains an optional feature. However, ADS–B transmits information over open and unencrypted protocols, so it can be easily compromised using existing hardware and software, which poses a major security risk. Thus, ADS–B can be exposed to different types of cyber attacks, such as eavesdropping, jamming and spoofing. As countermeasures to these attacks, various techniques are proposed, from cryptographic, to techniques that use location verification, to machine learning techniques (artificial intelligence). In addition to existing security solutions and protocols, the International Civil Aviation Organization (ICAO) and other organizations, working groups and conferences continuously analyze and monitor effective cyber countermeasures/methods and their integration into air traffic control, communication and navigation systems. Also, the approach to the problem of cyber security (especially ADS–B), apart from the technical-organizational base that represents a barrier, which prevents a cyber attack from penetrating to the aircraft/cockpit, also requires the integration of the human factor (aircraft crew/pilot) into the cyber-defense layer , or, what's more, for the pilot to be the last line of defense – because it is completely clear that human decisions based on previous knowledge and abilities are a necessity for overcoming/resolving critical situations. Although, according to ICAO's assessment, the risk of a successful cyber attack with the loss of human life, compared to other forms of terrorist attacks, is relatively low, nevertheless, most recently, there have been numerous cases of disruption of airline operations due to various cyber incidents, which, apparently of a small scale, but with an increasing tendency, they can have much wider and more

serious consequences. In this context, the aim of this dissertation is to investigate some of the main issues of cyber security in aviation, especially the ADS–B system, i.e. potential use of ADS–B vulnerabilities and their impact on aviation operations, then, a systematic qualitative and interpretive analysis of real cyber threats/incidents in civil aviation, as well as the application of ADS–B in the analysis of the most recently recorded incident situations in aviation. Also, the analysis includes the author's personal experience in the field of civil aviation, which contributes to a more comprehensive understanding of the problem.

Key words: ADS-B, GPS/GNSS, civil aviation, information-communication technology, security, vulnerabilities, cyber attack, terorism

Scientific field: Multidisciplinary, Interdisciplinary, Computer studies

Narrow scientific field: Computer studies

САДРЖАЈ

СПИСАК СКРАЋЕНИЦА И АКРОНИМА

1. **УВОД** 1

1.1. Проблеми истраживања 3
1.2. Предмет истраживања 4
1.3. Циљеви истраживања 7
1.4. Хипотезе истраживања 7
1.5. Методе истраживања 8
1.6. Очекивани резултати и научни допринос 9
1.7. План и структура рада 11

2. **САЈБЕР НАПАД И САЈБЕР БЕЗБЕДНОСТ** 13

2.1. Концепт сајбер напада 14
2.1.1. Дефинисање сајбер напада 14
2.1.1.1. Сајбер простор 14
2.1.1.2. Сајбер напад 19
2.1.2. Рањивости као кључни чиниоци сајбер напада 22
2.2. Концепт сајбер безбедности 32
2.2.1. Информациона и сајбер безбедност 33

3. **САЈБЕР БЕЗБЕДНОСТ ЦИВИЛНЕ АВИЈАЦИЈЕ** 37

3.1. Сајбер рањивости цивилне авијације 39
3.1.1. Цивилна авијација и информационо-комуникационе технологије 42
3.1.2. Кључне сајбер претње у цивилној авијацији 48
3.1.2.1. Контрола летења 52
3.1.2.2. Авион 56
3.1.2.3. Авиокомпаније 72
3.1.2.4. Аеродроми и пограничне власти 72

4. **УПРАВЉАЊЕ САЈБЕР БЕЗБЕДНОСНИМ РИЗИЦИМА** 80

4.1. Сајбер безбедносне стратегије 83
4.1.1. Правни и регулаторни оквир сајбер безбедности ваздухопловног система 88
4.1.2. Међународне организације и институције које се баве сајбер безбедношћу у авијацији 92
4.1.3. Сајбер безбедност у Европској унији и Србији 99

4.2. Методологија процене сајбер безбедности 107

5. **GPS/GNSS: ФУНДАМЕНТАЛНИ КОНЦЕПТ И САЈБЕР БЕЗБЕДНОСТ** 112

5.1. GPS/GNSS технологија 113
5.1.1. GPS/GNSS фундаментални концепт 116
5.1.1.1. GPS сигнали 121
5.2. САЈБЕР БЕЗБЕДНОСТ GPS/GNSS-а 125

5.2.1. Сајбер рањивости GPS/GNSS-а 128
5.2.1.1. Врсте безбедносних претњи на GPS/GNSS – *spoofing* у авијацији 130
5.2.2. GPS/GNSS стратегије за ублажавање сајбер рањивости 135
5.3. Примена фази логике за анализу параметара 141
5.3.1. Фази логика – основе концепција 142
5.3.1.1. Фази логички алгоритми за класификовање GPS сигнала – кратки преглед литературе 148

6. **ADS–B АВИО СИСТЕМ: АРХИТЕКТУРА И САЈБЕР БЕЗБЕДНОСТ** 151

6.1. ADS–B: Фундаментални концепт 154
6.1.1. ADS–B технологија 154
6.1.2. ADS–B инфраструктура и комуникациони протоколи 160
6.1.3. ADS–B подаци 165
6.1.4. ADS–B имплементација 170
6.1.5. Ефикасност ADS–B система 174
6.2. Сајбер безбедност ADS–B авио система 180
6.2.1. Врсте безбедносних претњи на ADS–B систем 181
6.2.1.1. Радио-фрекценцијске интерференције (RFI) 184
6.2.2. Заштита ADS–B од сајбер напада: безбедносна решења 189
6.3. Људски фактор у одбрани од сајбер напада 196

7. **АНАЛИЗА И ПРИКАЗ РЕЗУЛТАТА ИСТРАЖИВАЊА** 201

7.1. Примери реалних сајбер инцидената у цивилној авијацији 202
7.2. Примена ADS–B технологије: студије случаја 211
7.2.1. Фатална несрећа/нестанак малезијског авиона *Boeing* 777 212
7.2.2. Фатална несрећа етијопијског авиона *Boeing* 737-800 Max 218
7.3. Примери примене ADS–B у ваздушном саобраћају 224
7.3.1. Фатална несрећа кинеског авиона *Boeing* 737–800 (март, 2022) 224
7.3.2. Девијација путање лета UA1722 (децембар, 2022) 226
7.3.3. Понирање током процедуре полетања *Boeing* 787-8 (QR161) (јануар, 2023) 229

ЗАКЉУЧАК 233

ЛИТЕРАТУРА

БИОГРАФИЈА АУТОРА

СПИСАК ОБЈАВЉЕНИХ РАДОВА

ПРИЛОЗИ

Прилог 1 – Изјава о ауторству

Прилиг 2 – Изјава о истоветности штампане и електронске верзије докторског рада

Прилог 3 – Изјава о коришћењу

Прилог 4 – Потврда о одобравању коришћења ADS–B података

СПИСАК СКРАЋЕНИЦА И АКРОНИМА

AAIM	Aircraft Autonomous Integrity Monitoring
ABAS	Aircraft-Based Augmentation System
ACAS	Airborne Collision Avoidance System
ACARS	Aircraft Communications, Addressing and Reporting System
ACC	Area Control Centres
ACI	Aviation Cybersecurity Initiative
ACSS	Aviation Communication Surveillance Systems
ACAS	Airborne Collision Avoidance System
ADC	Analog-To-Digital Converter
ADS–B	Automatic Dependent Surveillance – Broadcast
ADS–B APT	ADS–B for Airport Surface Surveillance
ADS–B NRA	ADS–B in Non Radar Airspace
ADS–B RAD	ADS–B in Radar Airspace
ADS–R	Automatic Dependent Surveillance-Rebroadcast
AEEC	Airlines Electronic Engineering Committee
AFDX	Avionics Full DupleX Switched Ethernet
AFIS	Automated Fingerprint Identification System
AGC	Automatic Gain Control
AI	Artificial Intelligence
AIAA	American Institute of Aeronautics and Astronautic
AIP	Aeronautical Information Publications
ANF	Adaptive Notch Filters
ANFIS	Adaptive Neuro-Fuzzy Inference System
ALS	Alerting Service
AMAN	Arrival Manager
ANSP	Air Navigation Service Provider
AOA	Air Operations Area
AoA	Angle of Arrival
APT	Advance Persistent Threat
ARINC	Aeronautical Radio, Incorporated
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ARAIM	Advanced Receiver Autonomous Integrity Monitoring
ARTAS	ATM Surveillance Tracker and Server
ASAS	Airborne Collision Avoidance System
ASDE	Airport Surface Detection Equipment
ASEPS	Advanced Surveillance Enhanced Procedural Separation
ASISP	Aircraft Systems Information Security/ Protection
ASM	Air Space Management
ASSC	Airport Surface Surveillance Capability
ASPA–FIM	Flight Deck Interval Management
ASTERIX	All Purpose Structured Eurocontrol Surveillance Information Exchange
ATAS	ADS–B Traffic Advisory System
ATC	Air Traffic Control
ATFM	Air Traffic Flow Management
ATIS	Automatic Terminal Information Service
ATM	Air Traffic Management

ATN	Aeronautical Telecommunication Network
ATS	Air traffic services
ATSAW	Airborne Traffic Situation Awareness
ATSAW AIRB	ATSAW during Flight Operations
ATSAW ITP	ATSAW In-Trail Procedure in oceanic airspace
ATSAW SURF	ATSAW on the Airport Surface
ATSAW VSA	ATSAW Visual Separation in Approach
AWN	Avionics Wireless Network
BPSK	Binary Phase Shift Keying
BOC_{sin}	Binary Offset Carrier signals (sine-phase)
BYOD	Bring Your Own Device
BYOP	Bring Your Own Phone
BYOPC	Bring Your Own Personal Computer
CAPSCA	Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation
CARATS	Civil Aviation Reform of Air Traffic Services
CAVS	CDTI Assisted Visual Separation
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CDM	Cooperative Decision Making process
CDMA	Code Division Multiple Access
CDTI	Cockpit Display of Traffic Information
CDU	Control Display Unit
CERT-EU	Computer Emergency Response Team for the EU Institutions, bodies and agencies
CFIT	Controlled Flight Into Terrain
CIA	Central Intelligence Agency
COTS	Commercial-Off-The-Shelf
CPDLC	Controlled Pilot Data-Link Communication
CPR	Compact Position Report
CRPA	Controlled Reception Pattern Antenna
CSDP	Common Security and Defence Policy
CSMM	Call Sign Mismatch
CSV	Comma Separated Values
CWP	Control Working Position
DANFIS	Dynamic Adaptive Neuro-Fuzzy Inference System
DARPA	Defense Advanced Research Project Agency
DFMC	Dual-Frequency Multi-Constellation
DHS	Depatment of Homeland Security (USA)
DME	Distance Measuring Equipment
DNS	Domain Name System
DDoS	Distributed Denial of Service
DOD	Department of Defense (USA)
DoS	Denial-of-Service
DSCN	Digital Satellite Communication Networks
EACCC	European Aviation Crisis Coordination Cell
EASA	European Union Aviation Safety Agency

ECAC	European Civil Aviation Conference
EDR	Endpoint Detection and Response
EFB	Electronic Flight Bag
EFD	Electronic Flight Display
EFIS	Electronic Flight Instrument System
EFVS	Enhanced Flight Vision System
EGNOS	European Geostationary Navigation Overlay Service
ENISA	European Union Agency for Network and Information Security
ESA	European Space Agency
ETSI	European Telecommunication Standards Institute
EU	Europe Union
EUROCAE	European Organization for Civil Aviation Equipment
EUROCONTROL	European Organization for the Safety of Air Navigation
FAA	Federal Aviation Administration
FBI	USA Federal Bureau of Investigation
FBO	Fixed-Base Operator
FCS	Flight Control System
FDP	Flight Data Processing
FIM	Flight-deck Interval Management
FIR	Flight Information Region
FIS	Flight Information Service
FIS–B	Flight Information Service-Broadcast
FLC	Fuzzy Logic Controller
FLS	Field Loadable Software
FMS	Flight Management System
FPD	Frequency Power Detector
FRA	Free Route Airspace
FTA	Fault Tree Analysis
GAGAN	GPS-Aided GEO Augmented Navigation
GAO	Government Accountability Offis (USA)
GARIC	Generalized Approximate Reasoning-based Intelligent Control
GBAS	Ground-Based Augmentation System
GBT	Ground Based Transievers
GDOP	Geometric Dilution of Precision
GEO	Geostationary Earth Orbit
GFCE	Global Forum of Cyber Expertise
GNSS	Global Navigation Satellite System
GMT	Greenwich Mean Time
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
HEO	High Earth Orbit
HF	High Frequency
HUD	Head-up display
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICANN	Internet Corporation for Assigned Names and Numbers

ICT	Information Comunication Techologie
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronic Engineers (US)
IETF	Internet Engineering Task Force
IFE	In Flight Entertainment
ILS	Instrument Landing System
IM	Interval Management
INFOSEC	Information security
INS	Internal Reference System
IoT	Internet of Things
IP	Internet Protocol
IPS	Internet Protocol Suite
IRS	Inertial Reference System
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
ISP	Internet Service Provider
IT	Information Technology
ITP	In-Trail Procedures
ITU	International Telecommunication Union
KML	Keyhole Markup Language
LAN	Local Area Network
LDCAS	L-band Digital Aeronautical Communications Systems
LEO	Low-Earth Orbit
LOC	Lines of Code
LOS	Line Of Sight
LSTM	Long Short–Term Memory
LTE	Long Term Evolution
MAC	Media Access Control
MANET	Mobile Ad Hoc Networks
MAVPro	Massage Verification Protocol
MCAS	Maneuvering Characteristics Augmentation System
MDM	Mobile Device Management
MEO	Medium Earth Orbit
MFD	Multi-Function Display
MLAT	Multilateration
MLS	Microwave Landing System
MOPS	Minimum Operational Performance Standard
MRO	Maintenance, Repair and Overhaul
MSAS	Multi-functional satellite augmentation system
MSTFT	Modified Short Time Fourier Transform
MTCD	Medium-Term Conflict Detection
NAC	Network Access Control
NACp	Navigation Accuracy Category for Position
NACv	*Navigation Accuracy Category for Velocity*
NASA	National Aeronautics and Space Administration
NAS	National Airspace System

NATO	North Atlantic Treaty Organization
NAVSTAR	Navigation Satelite Timing and Ranging
NEFCON	NEuro-Fuzzy CONtrol
NextGen	Next Generation Air Transportation System
NFC	Near Field Communication
NIC	Navigation Integrity Category
NIST	National Institute of Standards and Tecnology (USA)
NLOS	Non-Line-Of-Sight
NM	Network Manager
NPE	Non Performing Emitter
NRZ – M kôd	Non-Return-to-Zero Mark kod
NRZ–L kôd	Non-Return-to-Zero Level kod
NSA	National Security Agency (USA)
NTSB	National Transportation Safety Board (USA)
OSCE	Organization for Security and Cooperation in Europe
PANET	Personal Ad Hoc Network
PBN	Performance Based Navigation
PBM	Pulse Blanking Methods
PCA	Principal Components Analysis
PDD	Personal Protection Device
PESCO	Permanent Structured Cooperation
PFD	Primary Flight Display
PID	Proportional Integral Derivative
PKI	Public Key Infrastructure
PLD	Power Law Detector
PNT	Position, Navigation, Time
PPS	Precise Positioning Service
PRN	Pseudo Random Noise
PSD	Power Spectral Density Function
PSR	Primary Surveillance Radar
PVT	Position, Velocity, Time
QR Code	Quick Response Code
RA	Resolution Advisory
RADAR	Radio Detection and Ranging
RAIM	Receiver Autonomous Integrity Monitoring
RATEL	Regulatorna agencija za elektronske komunikacije i poštanske usluge
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RNAV	Area Navigation
RPA	Remotely Piloted Aircraf
RPAS	Remotely Piloted Aviation Systems
RTCA	Radio Technical Commission for Aeronautics
RTS	Realtime computer System
RWY	Runway

SADIS	Satellite Distribution System
SARP	Standards and Recomended Practices
SatNav	Satellite Navigation
SBAS	Space Based Augmentation Systems
SBS	Surveillance and Broadcast Services
SCADA	Supervisory Control and Data Acquisition
SDA	System Design Assurance
SDR	Software Defined Radio
SESAR	Single European Sky Air Traffic Management Research
SFP	State Focal Point
SIDA	Security Identification Display Area
SMS	Safety Management System
SODA–DNN	Strategic Options Development and Analysis-Deap – Deep Neural Network
SPS	Standard Positioning Service
SSGC	Secretariat Study Group on Cybersecurity
SSR	Secondary Surveillance Radar
SSV	Space Service Volume
STCA	Short-Term Conflict Alert
STFT	Short Time Fourier Transform
SVM	Support Vector Machine
SWOT	Strengths, Weaknesses, Opportunities, Threats
TA	Traffic Advisory
TAO	Tailored Access Operations (danas, Computer Network Operations)
TBO	Trajectory-Based Operations
TCAS	Traffic Collision Avoidance System
TCP	Internet Transmission Control Protocol
TDoA	Time Difference of Arrival
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TICS	Transportion Industrial Control System
TIS–B	Traffic Information Service-Broadcast
ToA	Time of Arrival
TPD	Time Power Detector
TR	Transponder
TSA	Transportation Security Administration
TSAA	Situation Awareness with Alerting Application
TSV	Terrestrial Service Volume
UA	Unmanned Aircraft
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aerial System
UHF	Ultra high frequency
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
UNICEF	United Nations International Children's Emergency Fund
UNOPS	United Nations Office for Project Services

USB	Universal Serial Bus
USDOT	US Department of Transportation
UTC	Universal Time Coordinated
VENET	Vehicular Ad Hoc Network
VDB	Data Broadcast
VHF	Very high frequency
VPN	Virtual Private Network
VOR	VHF Omnidirectional Radio Range
VoR	Voice-over-the-Radio
WAAS	Wide Area Augmentation System
WAIC	Wireless Avionics Intra-Communication
WAM	*Wide Area Multilateration*
WAMLAT	Wide Area Multilateration
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WFMS	Wireless Flight Management System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WRLS	Weighted Recursive Least-Squares
1090ES/UAT	1090 MHz Extended Squitter/Universal Access Transceiver

СПИСАК СЛИКА

Слика 1. Слојеви и компоненте слојева сајбер простора
Слика 2. Однос информационе безбедности и сајбер безбедности
Слика 3. ICT окружење авио система; HW – хардвер; SW – софтвер
Слика 4. Пример *Glass cocpit*-а са *Primary Flight Display* (PFD) и *Multi-Function Display* (MFD) (а) и различити нивоа информација представљених на PFD и MFD (б и в)
Слика 5. Најважнији елементи функционисања *Traffic Alert and Collision Avoidance System*-а (TCAS): (а) ваздушни надзор (*airborne surveillance*), (б) безбедносна логика (*safety logic*), (в) вертикално раздвајање (*vertical advisories*) и (г) интерфејс с пилотом (*pilot interface*)
Слика 6. Транспаретни екран најновије технологије HUD (*Head-up display*) система за *Boeing* B737 са подацима
Слика 7. Сајбер безбедносне претње на авион; ILS – *Instrument Landing System*; ACARS – *Aircraft Communications, Addressing and Reporting System*; ADS–B – *Automatic Dependent Surveillance – Broadcast*; EFB – *Electronic Flight Bag*; FMS – *Flight Managment System*
Слика 8. Безбедносне области аеродрома (USA); TSA – *Transportation Security Administration*; SIDA – *Security identification display area*; AOA – *Air operations area*
Слика 9. Комуникациони интерфејси "ствари"
Слика 10. Врсте злонамерних претњи на сајбер безбедност паметног аеродрома
Слика 11. Сајбер-безбедносни оквир националне инфраструктуре – механизам заштите сајбер безбедности
Слика 12. Улоге и одговорности Владе, ваздухопловне индустрије и регулатора као партнера у успостављању сајбер безбедности
Слика 13. MRO (*Maintenance*, *Repair* и *Overhaul*) индустрија – SWOT анализа
Слика 14. Различити слојеви сајбер безбедности на аеродромима у доба експанзије BYOD-а
Слика 15. Архитектура GPS-а
Слика 16. GPS пријемник (*V*) користи навигационе сигнале $s_i(t)$ (i = 1–4) сателита (S_i, i = 1–4) за одређивање 3D положаја (*L*) и временског помака (δ) GPS пријемника
Слика 17. Позиција пријемника добијена решавањем система нелинеарних једначина (3)
Слика 18. Геометрија GNSS сигнала у гео-синхронизованој земаљској орбити (GEO)
1 – вектор (растојање од GNSS сателита до пријемника); 2 – вектор (растојање од GNSS сателита до центра Земље); 3 – правац тангенте GNSS сателита на вертикалу Земљине површине; *Umbra* – тамна, унутрашња сенка Земље, кружног попречног пресека
Слика 19. Дијаграм спектралне густине снаге сигнала L1 (а) и L2 (б)
PSD – *power spectral density function*
Слика 20. Структура GPS сигнала
Слика 21. Интерференције GNSS-а у случају напада са земље

Слика 22. Различите врсте спуфинга: (а) S1– Спуфинг понављањем и (б) S5– Циљани спуфери – Симулатори
Слика 23. Поједностављени блок-дијаграм типичног SatNav пријемника AGC – *Automatic Gain Control*; PVT – *Position, Velocity, Time*
Слика 24. Основне карактеристике фази скупова (граница, носач и језгро)
Слика 25. Графички приказ фази фунција припадности: (а) троугаона и (б) трапезоидна
Слика 26. *Charles Lindbergh* са супругом *Anne Morrow Lindbergh* (1932)
Слика 27. Шематски приказ: (а) *Primary Survaillance Radar* (PSR) и (б) *Secundary Surveillance Radar* (SSR)
Слика 28. Блок шема ADS–B система
Слика 29. Архитектура система ADS–B: ADS-B Out, ADS–B In, *Data link* и земаљских станица
Слика 30. Авионика система ADS-B Out (а) и ADS-B In (б)
Слика 31. Однос протокола режима транспондера и ADS–B протокола
Слика 32. ADS–B порука: структура проширене поруке дужине 112 бита
Слика 33. Блок дијаграм уграђене ADS–B опреме у авион (комуникацијски протокол 1090ES)
XPDR – транспондер; FMS – *Flight Management System*; WOW – *Weight On Wheels*; SBAS – *Space Based Augmentation System*; ADC – *Air Data Computer*
Слика 34. Еволуција опреме ADS–B (EU27+4): планирано опремање/уградња (тачкаста линија), планирано постепено укидање (испрекидана линија) и постојећа опрема (пуна линија), према CECAP-у
Слика 35. *Fault Tree Analysis* (FTA) анализа људских фактора ADS–B система
Слика 36. Класификација ADS–B напада према слојевима ADS-B протокола које компромитује (а) и безбедносних захтева (б)
Слика 37. Илустрација различитих врста спуфинг напада на ADS-B: напад са Земље (коришћењем SDR спуфера) и напад из ваздуха, тј. авиона (нападач користи ADS–B транспондер с измењеном ICAO адресом
Слика 38. Шематски приказ SODA–DNN методе за детекцију спуфинг напада на ADS–B систем
Слика 39. Карактеристике различитих порука, аутентична (а1) и малициозних (а2–а4) у нападима понављањем поруке (а2), понављањем IQ података (а3) и увођењем ″авиона-духа″ (а4)
Слика 40. Илустрација прикупљања података коришћењем ADS–B пријемника и спуфера базираног на SDR-у; ADS-B пријемник прикупља аутентичне поруке, које преноси SDR спуфер
Слика 41. Удео различитих врста сајбер напада на IT инфраструктуру сектора цивилне авијације
Слика 42. Малезијски авион *Boeing* 777 (MH370) који је мистериозно нестао 08. 03. 2014.
Слика 43. *Handshakes* трансмисије које је забележио сателит (08. 03. 2014)
Слика 44. Сматра се да је узрок пада авиона *Boeing* 737 Мах у Индонезији и Етијопији исти – неисправни сензор ″нападног″ угла

Слика 45. Функционисање *Maneuvering Characteristics Augmentation System* (MCAS)
Слика 46. Различита очитавања сензора (левог и десног) етијопијског авиона *Boeing* 737 MAX 8
Слика 47. Искључивање *Maneuvering Characteristics Augmentation System*, MCAS
Слика 48. Након приземљења авиона типа *Boeing* 737 Max, компанија *Boeing* ажурира софтвер MCAS-а и уводи још један AoA сензор
Слика 49. Приказ примарних информација о лету потребних за безбедно и ефикасно управљање 737 MAX; AoA индикатор даје додатне информације посади авиона
Слика 50. Мапа и путања лета *United Airlines*-а (flight UA1722), 18. децембра 2022. добијени на основу ADS–B података. Уметнута слика: графици брзине и надморске висине
Слика 51. Мапа и путања лета *Qatar Airways*-а (лет QR161), 10. јануар 2023. године, добијени на основу ADS–B података. Уметнута слика: графици брзине и висине
Слика 52. Мапа и путања лета *Qatar Airways*-а (лет QR161), 10. јануар 2023. године (графика: AVH/*Google Earth*

СПИСАК ТАБЕЛА

Табела 1. Различити извори сајбер претњи
Табела 2. Информациона безбедност, безбедност информационо-комуникационих технологија (ICT) и сајбер безбедност
Табела 3. Карактеристике комуникационих протокола ваздух–земља (VHF говорна комуникација, CPDLC и ACARS) и врсте потенцијалних сајбер претњи на комуникационе протоколе
Табела 4. Врсте радио-навигационих средстава (употреба, врста и опсег фреквенција)
Табела 5. Техничке карактеристике GPS фреквенцијских опсега L1, L2 и L5
Табела 6. Категоризација спуфунг напада
Табела 7. Упоредне карактеристике различитих ваздухопловних надзорних система (PSR, SSR, MLAT и ADS–B)
Табела 8. ASCII параметри (ASCII file: ADS-B transponder+call_sign+date and time.txt; frequency: 1Hz (10Hz)
Табела 9. Врсте, мотиви и начини сајбер напада на ADS–B систем
Табела 10. Преглед сајбер безбедносних инцидената у авијацији (1997–2023)
Табела 11. Преглед потенцијалних сајбер рањивости у авијацији (2008–2016)
Табела 12. Преглед сајбер безбедносних инцидената на аеродромима (2016–2023)
Табела 13. Авио-несрећа *China Eastern Airlines*-овог авиона *Boeing* 737–800 (B-1791, лет MU5735): пријављење ADS–B поруке, према *AirNav RadarBox*-у
Табела 14. Лет UA1722, авиона *Boeing* 777-200EP, *United Airlines*-а: пријављене ADS–B поруке, које обухватају временски период 00:50:37:759–00:51:11:250 UTC према *Air Current*-у
Табела 15. Лет QR161, авиона *Boeing* 787–8, *Qatar Airways*-а: пријављене ADS–B

поруке, које обухватају временски период 23:01:18Z.082–23:02:11Z.298 UTC на основу грануларног CSV-а (*Flightradar*24)

1. УВОД

"Авијација се у великој мери ослања на рачунарске системе у земаљским и летачким операцијама, као и управљању ваздушним саобраћајем, тако да знамо да смо мета." – *Tony Tyler, генерални директор* IATA *и* CEA (2011–2016)

У ери информационих и комуникационих технологија (ICT), функционисање сектора ваздухопловства, заснива се на интра- и интер повезивању рачунарских система; ова критична национална инфраструктура, у претходној деценији, веома је брзо искористила напредак дигиталне технологије у циљу повећања ефикасности кључних процеса као што су системи за руковање пртљагом на аеродромима и системи за приказ информација о лету, као и ICT за управљање различитим операцијама у ваздухопловству [1]. Међутим, ово повезивање утиче на то да инфраструктурни авио-системи постају рањиви на различите врсте сајбер напада, што представља велики безбедносни ризик. Наиме, ваздухопловна телекомуникациона мрежа јесте *ad-hoc* бежична мрежа која има велики број мобилних чворова, а ова мобилност, као најслабија карика у ланцу, може се искористити за предузимање потенцијалног сајбер напада [356].

Усвајање иницијатива за самоуслуживање путника, надоградње *Air Traffic Management* (ATM) технологија и бежичних *on-board* система за забаву путника, само су неки од илустрација свеприсутне дигитализације и оперативних бенефита који произилазе из примене технолошких алата и система конектованих на интернет. Међутим, на тај начин, сектор ваздухопловства све више "улази" у сајбер простор, чинећи да сајбер безбедност [2, 3] постане нови пејзаж за безбедност ваздухопловства. Тако, главни сајбер безбедносни изазови [4] односе се на ATM технологије, рачунарске мреже аеродрома и *e-enabled* авионе, а сектор авијације, требало би да се прилагоди овом новом амбијенту, тј. да омогући ефикасно решавање безбедносних изазова својствених огромној мрежи повезаних ваздухопловних технологија.

Сајбер безбедност у авијацији остварује се сарадњом националних агенција, приватних субјеката и међународних организација (нпр. *European Union Agency for Network and Information Security,* ENISA, *International Civil Aviation Organisation,* ICAO, *International Air Transport Association,* IATA, *European Organisation for Civil Aviation Equipment,* EUROCAE, итд.) [5]. При томе, од великог значаја је доношење адекватних (прилагођених актуелној ситуацији и захтевима) националних закона у вези са сајбер безбедношћу. Генерално, успостављање правног и регулаторног оквира за сајбер безбедносне стандарде и њихова примена, у фази је развоја, али је решавање различитих питања која се односе на сајбер безбедност у авијацији, неопходност [6].

С обзиром на предвиђања у вези с повећањем интензитета ваздушног саобраћаја, у годинама које долазе, кључно је одржати/побољшати усвојене стандарде безбедности и ефикасности у ваздухопловству. Због неопходности модернизације ATM-а (*Air Traffic Management*), покренута су два пројекта, и то,

Federal Aviation Administration (FAA) пројекат *Next Generation Air Transportation System* (NextGen) [7] и *European Organization for the Safety of Air Navigation* (EUROCONTROL) пројекат *Single European Sky Air Traffic Management Research* (SESAR) [8], у циљу ефикасног решавања различитих питања у вези с капацитетом ваздушног простора.

Саставни део ових пројеката је *Automatic Dependent Surveillance – Broadcast* (ADS–B), вишепараметарски систем за надзор, који је дизајниран за унапређење кључних сегмената ваздушног саобраћаја: омогућавање надзора у реалном времену, повећање безбедности и ефикасности, као и побољшање летачких и метеоролошких информација. Интегрални део ADS–B архитектуре [9–11], осим земаљске инфраструктуре и оперативних процедура, је *Global Positioning System* (GPS), односно *Global Navigation Satellite System* (GNSS), тако да ADS–B систем зависи од тачности система позиционирања. Према смеру преноса информација, систем функционише као ADS–B Out (основна функција уграђене ADS–B опреме, која шаље информације о положају авиона и додатне информације, према потреби, другим авионима/контролорима) и ADS–B In (опциона услуга која омогућава авиону да прима и приказује детаљне информације, а које емитују други авиони у околини). Иако само комплетан систем ADS–B In/Out омогућава бројне предности, као што су додатна свест о ситуацији и ефикасније океанско рутирање, FAA и *European Union Aviation Safety Agency* (EASA) захтеви односе се на ADS–B Out (обавезно увођење овог система надзора је било до јануара, односно јуна 2020. године), при чему ADS–B In остаје опциона функција.

Нема сумње да ће комплетан ADS–B In/Out систем бити у широкој употреби, али постоје одређене слабости – системи засновани на техникама сателитског позиционирања, као што су GPS/GNSS и ADS–B могу бити мета различитих сајбер напада. ADS–B има веома једноставан безбедносни протокол, који не обезбеђује релевантну енкрипцију (шифровање) и аутентификацију (потврђивање идентитета) података, што повећава рањивост овог система на различите врсте сајбер напада, као што су ометање и ускраћивање услуга (*jamming, denial of service*), прислушкивање (*eavesdropping*), убацивање/репродукција поруке (*message injection/replay*), манипулација порукама (*message manipulation*) и лажирања (*spoofing*) [12]. Овај последњи, веома је опасан и представља софистицирани облик радио-фреквенцијских сметњи (RFI) [13–15]. У *spoofing* нападу, предајник емитује лажне сигнале, који опонашају оригиналне сателитске сигнале; у односу на аутентичне, лажни сигнали имају већу снагу и различито временско кашњење. Уколико пријемник нема могућност разликовања лажних од оригиналних сигнала, пријемник се може "закључати" на лажне сигнале, тако да *spoofing* представља погодан начин за ефикасно преузимање система за позиционирање. Иако је експлоатација *spoofing-а* у цивилној авијацији на нивоу екцеса, техничка изводљивост лажирања GNSS и ADS–B система постаје све реалнија услед брзог напретка јефтиних SDR (*Software Defined Radio*) платформи. Такође, пораст употребе безпилотних летилица (*Unmanned Aerial Systems*, UAS)/дронова, отвара могућност њихове употребе за *spoofing* нападе из ваздуха у циљу отмице или дистракције безбедности у надзору ваздушног саобраћаја. Тако, у будућности, када

ће бројни UAS делити ваздушни простор с авионима са посадом, биће потребни нови концепти навигације и контроле летења [16].

Иако различити делови авио-система могу бити изложени сајбер нападима, а потенцијално и нападу лажирања, сектор авијације није безобзирно изложен сајбер нападима без одбране. Напади могу бити ублажени применом различитих против-мера за сајбер безбедносну заштиту (применом нпр. криптографских техника [17], као и различитих некриптографских приступа [18], и најскорије, метода које се заснивају на алгоритмима машинског учења, као што је модел дубоког учења, тј. вештачке интелигенције [19]. Такође, и пилоти су оспособљени да детектују и решавају проблеме у свакој фази лета. Међутим, због могућих софистицираних облика сајбер напада, међународне организације, као нпр. ICAO и EUROCAE, проактивно се баве повећањем робусности GPS/GNSS/ADS-B система на RFI и лажирање [20].

Иако се сматра да је ризик од успешног сајбер-напада на авио-системе, у односу на друге облике тероризма, релативно низак, имајући у виду садашњи ниво развоја информационих технологија, чињеница је да ће њихова учесталост у будућности бити све већа и да могу имати велики утицај на безбедност, оперативни и финансијски интегритет, као и углед авио сектора у целини, као и довести до потенцијалних катастрофа – сајбер напади/инциденти, иако малог обима, могу озбиљно угрозити оперативност авиоко-компанија, као и имати и далеко шире и озбиљније последице. У том контексту, веома је важна анализа сајбер безбедносних претњи, с нарочитим освртом на познате/доступне примере с којима се већ суочио/суочава авио сектор, а који илуструју свеприсутност сајбер инцидената и њихов утицај на авијацију, као и релеватност ове дисертације .

Такође, циљ ове дисертације је истраживање могућности искоришћавања и утицаја ADS–B рањивости на ваздухопловне операције – кроз одабране примере дата је квалитативна и интерпретативна анализа рањивости авио-система, нарочито ADS–B система, у циљу систематског приказа свих релевантних чињеница и околности које су у вези са проблемом истраживања и разумевања различитих аспеката и начина утицаја сајбер напад на пилота, као интегралног дела оперативности и контроле авиона.

Све већа доступност телеметријских података, које омогућава ADS–B систем, мотивисали су њихову употребу у различите сврхе, као нпр. процени атмосферских емисија из авиона класификоване по регионима, типовима авиона или хемијским врстама [21] и детаљној анализи инцидентних ситуација у авијацији [22]. Ово последње, дато је у дисертацији, кроз анализу одабраних реалних примера и користећи јавно доступне ADS–B податке добијене од комерцијалног сервиса Flightradar24.

1.1. Проблеми истраживања

Као нови ризик и изазов за безбедност цивилног ваздухопловства, идентификован је проблем сајбер безбедности.

Ваздухопловна индустрија, као једна од критичних националних инфраструктура, захтева веома висок ниво свих слојева безбедности и

имплементацију високих индустријских безбедносних стандарда. Иако прати напредне ICT и веома брзо их усваја, и то углавном безбедно, свако ново побољшање корисничких сервиса/повећање ефикасности авио операција, отвара простор за деловање сајбер криминалаца у циљу искоришћења нове/унапређене технологије, за личну, а понекад и политичку добит.

ADS–B систем је нова паридигма контроле летења и не захтева мануелне операције – омогућава аутоматско добијање параметара, као и емитовање/слање информација о статусу лета, како другим авионима, тако и земаљским станицама контроле летења. ADS–B се састоји од два субсистема, ADS–B Out и ADS–B In, који се односе на комуникацију између авиона и Земље (ADS–B Out) и међусобну комуникацију између авиона (ADS–B In). Крајњи рок за имплементацију ADS–B Out била је 2022. година, док ADS–B In и даље остаје опциона функција. Поред бенефита које нуди, главна критика ADS–B односи се на то што овај систем има веома једноставан *"free to air*" протокол који је рањив на различите сајбер-физичке нападе. Свакако, увођење ADS–B-а као глобалног стандарда у комерцијалном ваздухопловству, представља гигантски корак у модернизацији и побољшању квалитета ваздухопловних операција.

Основна питања која следе су:

– Који су изазови ове модернизације?
– Како искоришћавање рањивости ADS–B може довести до критичне ситуације?
– Да ли је отворена критика и бављење темом модернизације тривијално и постоје ли начини да се елиминишу сајбер рањивости ADS–B система?

Поред ових, а с обзиром да је сада ADS–B Out регулатива, важна питања су и следећа:

– Због чега је, неколико година након ступања на снагу мандата, систем ADS–B и даље тема, да ли су идентификовани проблеми и који су најновији изазови и могућности?
– Која су очекивања и да ли ADS–B нуди бенефите авио-компанијама након мандата?
– Да ли су пилоти и контролори летења, као крајњи корисници, довољно укључени и едуковани о свим аспектима функционисања ADS–B система, а посебно да ли су упознати с могућим безбедносним изазовима, тј. сметњама, којима могу бити изложени, као и адекватним против-мерама?

1.2. Предмет истраживања

Предмет истраживања ове дисертације јесте анализа сајбер безбедности ADS–B авио система. Информационо-комуникационе технологије су од кључног значаја за све гране друштва и нације, а њихов констатни развој повезан је с авијацијом на сваком нивоу, од побољшања система за праћење, навигацију и комуникацију, преко апликација, које користе пилоти за примање, складиштење и приказивање релевантних информација неопходних за доношење одлука у кокпиту, до ICT решења за продају авио карата и забаву путника током лета.

Од почетка 21. века, авијација се налази у процесу континуиране трансформације. Модернизацији и јачању авио система кроз побољшања и иновације у дизајну, технологији и ефикасности, супротставља се, често неприметна, рањивост у сфери сајбер безбедности. Свеприсутна дигитализација, као и технолошки алати и системи, који су најчешће повезани са интернетом, изложени су сајбер нападима и представљају озбиљан ризик за сајбер безбедност.

Увођење бежичног комуникационог протокола ADS–B, пружа бројне бенефите – аутоматизована размена информација између ваздухоплова и контроле летења без утицаја пилота и контролора, значајно утиче на аутономност и ефикасност летења, а тако и на уштеду ресурса. Међутим, главни недостатак ADS–B система у вези је са сигурносно/безбедносним аспектом, тј. чињеницом да ова инфраструктура има веома једноставан безбедносни протокол, који не обезбеђује енкрипцију (шифровање) и аутентификацију (провера идентитета) података, што повећава рањивост ADS–B система на различите врсте сајбер напада.

У предмету истраживања који се односи на анализу рањивости ADS–B и различитих сценарија сајбер напада на овај авио систем, као и предложених метода/техника за детекцију и ублажавање напада, веома је корисна њихова класификација и разматрање специфичности одређених врста напада. При томе, за разлику од напада са земље, потенцијални напади који би се могли остварити из ваздуха употребом беспилотних летилица/дронова у циљу отмице или дистракције у надзору ваздушног саобраћаја, још увек су недовољно испитани. Дефинисање чиниоца и сценарија нарушавања безбедности, омогућава квантификацију и потврда је директне повезаности степена заштите података и безбедности авио система.

У предмету истраживања, који се односи на примере реалних сајбер напада/инцидената на ADS–B систем, сагледавање њиховог утицаја на ваздухопловни систем је комплексно, а с обзиром на међузависност сложених авио система и њихове интеграције у авио компаније, што ствара услове у којима се ефекти сајбер напада, на једноставан начин, шире/преливају из једног система на други. С друге стране, поред пријављених сајбер инцидената, несумњиво постоје и они, који нису јавно објављени.

Природа сајбер напада је динамична и непредвидива, а ове нападе користе сајбер преступници у циљу остваривања различитих оштећења у ваздухопловном систему, а која у крајњем исходу могу угрозити, како људске животе, тако и функционисање авио сектора у целини. Очекује се константан пораст сајбер инцидентних ситуација услед веома брзог напредка јефтиних SDR *(Software Defined Radio)* платформи и развоја софистициранијих уређаја за извођење сајбер напада, тако их чинећи доступнијим и реалнијим. Нарочито, ризик представљају поменути сајбер напади који би се могли остварити употребом беспилотних летилица/дронова. Због свега тога, нови концепти навигације и контроле летења биће неопходни у ситуацији "препуног неба", где ће милиони дронова делити ваздушни простор са ваздухопловима с посадом и путницима.

Посебну врсту потенцијалних сајбер напада могу представљати злонамерни напади који софистицарано мењају тј. деградирају параметре и податке који

наизглед нису проблеаматични, али који у детаљнијој анализи заједно дају лажну слику неког процеса, команде или одлуке који се дешава у реалном времену. Овој врсти напада могу бити изложени, поред осталих и ADS–B системи.

Авио-индустрија, као и регулатори, сајбер ризике разматрају врло озбиљно и проактивно се баве повећањем робустности ADS–B система на различите врсте сајбер напада. Предмет овог истраживања је и разматрање регулативно-правног оквира сајбер безбедности, значај утврђивања сајбер безбедносних стратегија, као и методологије процене сајбер безбедности. Иако превентивне активности које се предузимају на нивоу држава, као и напори различитих агенција, конференција, као и организација на европском и глобалном нивоу минимизирају ризике, неопходно је задржати висок ниво свести о могућем, будућем развоју сајбер претњи на авио систем.

Предмет ове докторске дисертације је и разматрање ублажавања/минимизирања сајбер ризика узимајући у обзир људски фактор, тј. пилоте суочене са сајбер нападом. Оваквих истраживања, за разлику од оних која се односе на стратегију техничке одбране од сајбер напада, има релативно мало, али су веома сврсисходна. Инкорпорирање *cyber-awareness* у периодичну обуку пилота, омогућава развој поступака и техника обуке пилота за правовремено откривање и идентификацију сајбер напада, као и ефикасну реакцију на напад.

Просторно, временско и дисциплинарно одређење предмета истраживања:

Истраживање обухвата, у највећем уделу период од 2005. године, и нарочито од 2010. године до данас. Просуђивање о сајбер безбедности авио система ADS–B, неоствариво је без разумевања сајбер рањивости авио ситема, односно појма сајбер простора (*cyberspace*), које има глобални значај, и нема просторне границе. Просторно одређење предмета истраживања обухвата доступне податке/искуства и мере које су предузете/предложене на међународном нивоу, а у ужем смислу везано је и за територију Републике Србије.

Предмет истраживања докторске дисертације је разматрање технички оријентисане природе сајбер напада на ADS–B авио систем, као и актуелних приступа који се доминантно заснивају на техничким аспектима минимизирања сајбер напада. Поред неопходности постављања јаких техничких и организационих баријера за отклањање сајбер безбедносних ризика, у ланац одбране од сајбер напада, неопходно је интегрисати и човека, тј. пилота или контролора, као последње линије одбране. Шта више, анализа укључује лично искуство аутора у области цивилног ваздухопловства, што доприноси свеобухватнијем разматрању проблема. Приступ истраживању је мултидисциплинаран: заснива се на анализи и синтези из угла различитих научних дисциплина и примењених вештина значајних за предмет и садржај, међу којима су компјутерске науке, информационо-комуникационе технологије, информациона безбедност, организационе и правне науке.

1.3. Циљеви истраживања

Научни циљ истраживања ове дисертације је мултидисциплинарна анализа и систематизација досадашњих теоријских и јавно доступних практичних знања и искустава из области сајбер безбедности ADS–B авио система, у циљу дефинисања кључних категорија од значаја за разумевање сајбер сигурності/безбедности овог авио система.

Главни циљ истраживања је верификација ефеката имплементације сајбер безбедносних протокола, метода и техника за ублажавање сајбер напада на ADS–B авио систем, кроз прикупљање и опис реалних и сценарија потенцијалних сајбер инцидената ADS–B авио система. Овај истраживачки рад, анализом рањивости ADS–B система, подстиче проактивни однос према сајбер безбедносним питањима у авијацији, као и указује на значај константног задржавања високог нивоа свести о могућем, будућем развоју сајбер претњи/напада, с обзиром на то да исте могу имати велики утицај на безбедност, оперативни/финансијски интегритет и углед ваздухопловног сектора у целини, а у крајњој консеквенци могу довести и до губитака људских живота.

Посебан циљ рада је да се детаљно и свеобухватно прикаже и анализира актуелно стање у области сајбер безбедности ADS–B авио система – идентификација сајбер безбедносних претњи и рањивости, методологија процене сајбер рањивости, као и сајбер безбедносне стратегије. У одабраним примерима дата је квалитативна и интерпретативна анализа рањивости авио-система, нарочито ADS–B система, у циљу систематског приказа свих релевантних чињеница и околности које су у вези с проблемом истраживања – нарочито, одредити у којој мери и како технолошки напредак и аутоматизација утичу на сајбер безбедност ваздухопловног система, као критичне националне инфраструктуре, као и, што је веома важно, разумети различите аспекте и начине утицаја сајбер напада на пилота, као интегралног дела оперативности и контроле авиона.

1.4. Хипотезе истраживања

Општа хипотеза истраживања је следећа:

Уколико се авио систем модернизује, као што је прелазак на ADS–B бежични комуникациони протокол, тј. уводе нове информационо-комуникационе технологије и алгоритми за анализу угрожености система, онда се креирају нова безбедносна питања и изазови, који су у вези са сајбер безбедношћу.

Посебне хипотезе истраживања су следеће:

X1: Што је систем комплекснији, као што је авио индустрија, која се базира на међусобном (интер- и интра) повезивању информационо-комуникационих технологија, онда је изложенији сајбер нападима.

X2: Што је шири спектар начина извођења сајбер напада, с веома специфичним концептом угрожавања интегритета авијације, онда је сајбер безбедносним претњама у већој мери изложен целокупни авио систем, од система контроле летења, авиона и авиокомпанија, до аеродрома и пасошке/царинске контроле.

X3: Ако се користи најнапреднија технологија надзора у авио индустрији, тј. ADS–B систем, онда се поред бројних бенефита, могу очекивати и одређени недостаци, који су доминантно у вези с недовољном заштитом ове инфраструктуре и отвореношћу за сајбер нападе.

X4: Што су сајбер напади/претње у авијацији у већем порасту, динамичније и непредвидљивије, онда њиховом применом, сајбер преступници могу остварити различита оштећења у ваздухопловном систему, и то свих његових делова и система, као што су GPS/GNSS и ADS–B авио системи.

X5: Због нежељених и опасних последица које може имати на функционисање авио саобраћаја, веома је важно анализирати утицај потенцијалних сајбер напада на ADS–B.

X6: Уколико је неопходно одржавање сигурног и безбедног функционисања ADS–B система, као и целокупног авио сектора, отпорног на сајбер ризике, онда је потребно развијање сајбер безбедносних стратегија и високих сајбер безбедносних стандарда алгоритама и метода, као и њихова примена.

X7: Што су сајбер напади комплекснији и вишедимензионалнији, то је за научно истраживање одрживог модела процене/регулације сајбер безбедности ADS–B система, неопходнији мултидисциплинарни и интердисциплинарни приступ.

1.5. Методе истраживања

Методе које ће се користити у истраживању су **основне научне методе истраживања**, и то:

– аналитичка
– дескрипција
– метода студије случаја
– предикција
– синтеза
– индуктивно-дедуктивна
– оперативне методе (ретроспектива и анализа докумената)

Аналитичка метода ће омогућити, анализом основних категорија, дефиниција, прикупљених података и информација, као и постојећих регулатива, дубље разумевање сајбер безбедности ADS–B авио система, а с обзиром на комплексну и међусобно зависну природу посебних категорија од значаја за сајбер безбедност овог система.

Дескрипција ће омогућити, кроз приказе и описе конкретних примера сајбер претњи/инцидената са којима се суочава авијација данас, њихово боље разумевање, као и контролу и очекиване трендове у будућности.

Метода студије случаја биће примењена у циљу прикупљања података, анализе и утврђивања најбоље праксе и смерница/трендова развоја модела ублажавања/одбране од сајбер напада на авио системе.

Предикција нежељених сценарија са циљем валидације предложених алгоритама за анализу деградације и насилне промене појединих параметара посматраних комуникационих система.

Синтеза ће бити примењена при мултидисциплинарно оријентисаном дефинисању природе најважнијих категорија/појмова, у циљу сагледавања целокупности подручја сајбер безбедности при утврђивању карактеристичних својстава сајбер безбедности ADS–B авио система.

Индуктивно-дедуктивна метода ће бити примењена у току и након анализе сајбер безбедности ADS–B система у циљу процене постављених хипотеза истраживања и формирања закључака неопходних за остваривање циља истраживања.

Оперативне методе ће омогућити, кроз мултидисциплинарни приступ, тј. комбинацијом теоријских приступа и техника истраживања, добијање података релевантних за анализу ефективног алгоритма за идентификацију/детекцију фактора сајбер рањивости, релативних ризика и последица фактора ризика на безбедност ADS–B авио система. **Ретроспектива и анализа докумената** ће се користити за прикупљање података и анализу дефиниција, научних публикација, докумената и информација у циљу сагледавања степена угрожености ADS–B система и постојећих метода/техниха и регулатива за решавање сајбер безбедносних питања.

1.6. Очекивани резултати и научни допринос

Од ове дисертације **се очекује** да:

- систематизује савремена сазнања о ADS–B технологији, рањивостима ADS–B система, као и утицају сајбер напада на ADS–B, а што је донекле лимитирано ограниченим приступом документима (релативно висок ниво поверљивих информација), релативно малим бројем доступних информација (имплементација ADS–B у комерцијалну цивилну авијацију је завршена у јуну 2020. године), као и законским ограничењима примене реалних сајбер напада у циљу емпиријске процене ефеката на авио систем
- прецизно дефинише кључне сајбер безбедносне рањивости ADS–B система, тј. доминатне факторе и изворе сајбер напада на овај авио систем, као и односе између ваздухопловне, информационо-безбедносне и међународно-правне праксе
- сагледа процене авио-експерата и стручњака који се баве питањима сајбер безбедности у вези са отклањањем недостатака ADS–B авио система и њихове повратне информације
- потврди да широка употреба IoT (*Internet of Things*) уређаја, као и примена јефтиних SDR картица и сл., утиче на пораст рањивости, али и на велики значај развијања сајбер безбедносне заштите ADS–B авио система
- утврди/укаже на важност обуке и припреме пилота за идентификацију и правовремену реакцију на сајбер напад и подржи препоруке истраживача из области сајбер безбедности да се *cyber-awareness* инкорпорира у

периодичну обуку пилота (сајбер напади тренутно нису предмет обуке саобраћајних пилота)
- дефинише индикаторе на основу којих се може анализирати и квантификовати стање безбедности ADS–B авио система у односу на степен заштите података
- анализира предложена решења и закључке на бази претпостављених сценарија угрожености ADS–B система
- истакне и укаже на бенефите имплементације ADS–B система, нарочито расположивости велике количине ADS–B података у различитим анализама, а које омогућавају решавање бројних сложених проблема у пракси, као што је анализа инцидентних ситуација у авијацији.

Циљ ове дисертације је садржан у идентификацији природе кључних фактора значајних за сајбер безбедност ADS–B система и извора сајбер напада на овај авио-систем, као и односа између ваздухопловне, информационо-безбедносне и међународно-правне праксе. Из тог циља проистиче и **научни/практичан** допринос дисертације, који се огледа у **закључцима** истраживања. Један од закључака је да сајбер напади на ADS–B авио систем имају широке могућности примене, који примарно зависе од брзине развоја информационо-комуникационих технологија, а не од става авио индустрије и регулатора. Затим, ово истраживање је потврдило/утврдило да ADS–B пријемници могу детектовати сајбер нападе претраживањем аномалија у сигналу или користећи сигнале који су тако дизајнирани да спрече сајбер напад, а напредне технологије за ублажавање радио фреквенцијских (RF) интерференција користе алгоритме за обраду сигнала. Актуелни модели сајбер безбедносне заштите ADS–B система, приказани кроз анализу постојећих сајбер безбедносних метода/техника, могу мотивисати/помоћи стручњацима и научницима из области сајбер безбедности да, у складу са специфичностима истраживања, примене одговарајуће безбедносне моделе, као и усмерити даља истраживања из ове области. Такође, анализом сајбер напада, се истиче/доказује да су главне претње у сектору цивилне авијације у вези су с хакерским групама, које делују у сарадњи са одређеним државним актерима, у циљу крађе интелектуалне својине и поверљивих података како би унапредили своје ваздухопловне способности, као и надгледали, инфилтрирали и вршили субверзивне активности. Остали закључци односе се на правце развоја сајбер-безбедносних стратегија и начине њихове имплеметације у авио систем. Истраживањем се утврђује да једино правовремено реаговање на могућност компромитовања значајних података може спречити угрожавање безбедности ADS–B, као и авио система у целини. У том контексту, од посебног значаја је управљање сајбер безбедносним ризицима и предузимање одговарајућих мера заштите, затим, ефикасно реаговање и опоравак од сајбер инцидента, као и промовисање културе безбедности мрежа и података, подизање свести о информационој безбедности и изградња адекватне сајбер архитектуре. Такође, у дисертацији је утвђено да ублажавање/минимизирање сајбер рањивости није могуће остварити базирајући се само на техничким аспектима безбедносне заштите, већ је неопходно, у одлучујући/последњи ниво сајбер одбране, интегерисати оператера, тј. пилота/контролора. У том смислу, један од закључака дисертације

јесте указивање на неопходност инкорпорирања *cyber-awareness* у периодичну обуку пилота у циљу правовременог откривања и идентификације сајбер напада, као и ефикасну реакцију пилота на сајбер напад. Такође, резултати представљени у овом раду у великој мери имају бенефите од транспарентности, поновљивости и једноставности ажурирања ADS–B података, тако да се у закључку истиче да се поред коришћења ових отворених података за надзор лета авиона (нарочито у инцидентним ситуацијама), појављују и нове могућности за различита моделирања заснована на подацима о лету авина, као што је нпр. предвиђање перформанси или моделирање потрошње горива.

Допринос конкретној науци:

- Ова дисертација доприноси компјутерским наукама и областима примене информационо-комуникационих технологија, јер разматра техничко-технолошки оријентисану природу сајбер напада на ADS–B авио систем, као и приступе који се базирају на техничким аспектима безбедносне заштите овог система.
- Допринос ове докторске дисертације је и у областима организационих наука и информационе безбедности, и то у сегментима који се односе на методологију процене сајбер рањивости авио система, тј. процену угрожености или тестирања на бази реалних сценарија, као и информационо-безбедносне стратегије, које се морају развијати и континуирано унапређивати, због веома брзе еволуције сајбер напада, а под утицајем развоја и примене нових технологија у авио сектору

Очекује се друштвени допринос ове докторске дисертације у следећем:

- допринос бољем разумевању неопходности правовременог реаговања и опоравка од сајбер инцидента и изградњи адекватне сајбер архитектуре
- промовисању културе безбедности мрежа и података
- подизању свести о информационој безбедности
- допринос мотивацији научника и стручњака за сајбер безбедност да интензивирају истраживања из ове области
- допринос спознаји потребе регулаторних тела на националном ниву, који се баве безбедносном питањима у авијацији, за постављањем јасних смерница и постављања/прихватања нових стандарда за следећу генерацију авионике

1.7. План и структура рада

Циљ рада је квалитативна анализа утицаја сајбер претњи на ADS–B авио систем, као и на безбедност авио-система у целини, у циљу сагледавања и бољег разумевања начина за превазилажење сајбер инцидентних ситуација, а на основу јавно доступних практичних знања и искустава из области сајбер безбедности.

Дисертација је организована на следећи начин:

- Поглавље 1. Увод – даје опште објашњење теме и сврху истраживања дисертације.
- Поглавље 2. Сајбер напад и сајбер безбедност – обухвата појмновно одређење сајбер простора и сајбер напада, као и рањивости као кључних чиниоца сајбер напада.
- Поглавље 3. Сајбер безбедност цивилне авијације – обухвата појмновно одређење сајбер безбедности у ваздухопловству, тј. дефинисање и разумевање рањивости цивилне авијације на различите врсте сајбер напада, при чему је сајбер-безбедносним претњама изложен целокупни авио систем, од система контроле летења, преко авиона и авиокомпанија, до аеродрома и пасошке/царинске контроле.
- Поглавље 4. Управљање сајбер безбедносним ризицима – даје основе сајбер безбедносне стратегије у ваздухопловству, нарочито у Европској Унији и Србији и истиче неопходност постављања правног и регулаторног оквира за сајбер-безбедносне стандарде и њихову примену, кроз партнерски однос националних регулатора, међународних организација и заинтересованих приватних субјеката.
- Поглавље 5. GPS/GNSS: фундаментални концепт и сајбер безбедност – описује фундаментални концепт GPS/GNSS технологије, рањивости и различите врсте сајбер напада на GNSS, затим, примену различитих методологија за процену сајбер-безбедносних ризика GNSS-а, као и нових праваца у анализи GPS података (методе фази система закључивања, као и нових фази алгоритама за класификовања података и примена у области авијације).
- Поглавље 6. ADS–B авио систем: архитектура и сајбер безбедност – описује основе ADS–B система (технологију, тј. инфраструктуру, комуникационе протоколе, имплементацију и ефикасност) и различите начине потенцијалног напада на ADS–B, затим, разматра неке аспекте односа између ADS–B система и људског фактора, као и улога људског фактора у одбрани од сајбер напада; бави се и изазовима у примени ADS–B, као и будућим правцима развоја ADS–B у контексту оквира за модернизовани ваздухопловни систем.
- Поглавље 7. Анализа и приказ резултата истраживања – даје систематизацију и квалитативну анализу реалних сајбер претњи/инцидената у цивилној авијацији (засновану на научним радовима, званичним ваздухопловним документима, извештајима базираним на *web*-у и новинским чланцима) и примену ADS–B (студије случаја – нестанак малезијског авиона *Boeing* 777 (MH370), затим, описује карактеристичан случај у вези са сајбер рањивостима *e-Enabled* авиона (студија случаја – фатална несрећа *Boeing* 737 MAX 8), као и примену ADS–B података у детаљној анализи најскорије евидентираних инцидентних ситуација у ваздухопловству кроз анализу одабраних реалних примера.
- Закључак – ово поглавље истиче резултате анализе и даје додатну дискусију у вези с резултатима истраживања и препорукама.

2. САЈБЕР НАПАД И САЈБЕР БЕЗБЕДНОСТ

"Глобална дигитална инфраструктура подупире скоро сваки аспект савременог друштва, мењајући парадигму у размени информација. Оно што ову промену чини посебном, осим брзог технолошког развоја, јесте и ниво глобалне међусобне повезаности система и мрежа без преседана. Сведоци смо константног пораста сајбер напада на све секторе. Ваздухопловство није изузетак, а оно што карактерише овај систем, су широка међуповезаност и сложеност, висок ниво медијске пажње, као и критична улога у друштвено-економском развоју државе." [23]

Значајан развој информационо-комуникационих технологија (ICT) у протекле две деценије, имао је и велике импликације на све области друштва – ICT се сматра кључним фактором привредног и друштвеног развоја једне државе, јер има позитивне ефекте на економски раст, продуктивност и запосленост [24].

Информационо-комуникационе технологије представљају проширење термина информациона технологија (IT), тако истичући интеграцију рачунарских система и телекомуникација у циљу да корисницима омогући приступ, складиштење, пренос и обраду информација [25]. ICT и IT се, у највећем обиму, заснивају на **рачунарским технологијама** (најчешће дигитални системи, али могу бити и аналогни, као и квантни рачунарски системи), које омогућавају аутоматску обраду података [26]. ICT је скуп технологија, које се користе за руковање телекомуникацијама, електронским медијима, интелигентним системима за управљање зградама, аудиовизуелним системима за обраду и пренос, итд. Обухвата и средства масовне комуникације (радио, телевизија, телефонија, интернет), рачунарске системе (хардвер и софтвер) и најсавременије ICT компоненте (вештачка интелигенција и роботика) [27]. **Информационе технологије**, као подскуп ICT, су технологије, које за складиштење, анализу, преузимање, дистрибуцију и обраду података и информација, користе рачунарске системе (хардвер и софтвер) и рачунарске мреже, често у контексту пословања ограничене групе корисника.

Незаустављив и веома брз развој ICT, с друге стране, креира и нове опасности и претње, које се генеришу у окружењу које егзистира и функционише на основу примене рачунарских информационих технологија, тј. у сајбер простору. **Сајбер напади/претње** (део 2.1.) генерално представљају акте агресије у **сајбер простору**, или кроз сајбер простор, на информациони систем другог ентитета. Специфичне су природе, а злонамерни чиниоци (сајбер преступници), користе сајбер простор, као нову тактику и оружје у циљу остваривања различитих циљева (урушавање државних ICT, шпијунажа, финансијска злоупотреба, криминал и сл.), тако угрожавајући државе, корпорације и појединце. Због тога, очување и просперитет свих сегмената друштва, умногоме зависи од **сајбер безбедности**, односно **информационе безбедности** у сајбер простору, а чији је крајњи циљ оспособљавање власника/корисника информационих система/информација за одбрану/заштиту од различитих врста сајбер напада (део 2.2).

2.1. КОНЦЕПТ САЈБЕР НАПАДА

Непрестани, динамички развој ICT[1] и њихова примена у готово свим сферама људске делатности, унапређује и начин функционисања људског друштва – од начина комуникације и рада, до размене и приступа информацијама, садржајима, сервисима и услугама [29]. Као главни генератор промена у савременом свету, ICT су катализатор, као и један од главних разлога за настанак глобализације [30], као и концепта информационог друштва[2] [32]. Међутим, развој и употреба ICT детерминише и безбедносне ризике, што се нарочито односи на **сајбер нападе/претње** (делови 2.1.1 и 2.1.1.2), који се остварују у **сајбер простору** (део 2.1.1.1). Суштина постојања сајбер напада је искоришћење недостатака/грешака, тј. **рањивости** (део 2.1.2.) у техничким (хардвер), софтверским и информационим системима. Дакле, сајбер простор[3] представља ново подручје сукоба/напада, а због својих карактеристика, и нарочито, брже комуникације, доступности великој количини информација у реалном времену, као и могућности анонимности актера, налажење ефективних против-мера сајбер нападима, у многим случајевима, веома су изазовне. При томе, у обезбеђивању сајбер безбедности, тј. заштити виталних интереса личности/грађана, друштва и државе при коришћењу сајбер простора, веома је важан развој и усвајање стратегија сајбер безбедности, како на националном, тако и глобалном нивоу [33–36].

2.1.1. Дефинисање сајбер напада

Примена ICT креира **сајбер простор** (део 2.1.1.1), специфично и ново подручје људског деловања, па тако и оног, које се предузима у циљу наношења штете компјутерским системима. Поред ових планираних, и непланиране (ненамерне) активности проузроковане системским (софтверским) грешкама/недостацима у дизајну, или временским непогодама, представљају претњу у области сајбер безбедности. У **сајбер нападу**/сукобу (део 2.1.1.2) постоје технолошке специфичности и ограничења, која се односе на веома тешко правовремено детектовање сајбер напада, немогућност атрибуције нападача, као и одређивања одговорности за предузети напад. За разумевање концепта сајбер напада, потребно је разумети значења и дефиниције појмова у вези са сајбер простором, а који настају применом ICT и мењају се с константним развојем ICT.

2.1.1.1. Сајбер простор

Синтагма сајбер простор (*cyberspace*) настала је у USA, и овај израз је, веома брзо и упоредо са развојем/применом ICT, усвојен у целом свету. Претеча концепта

---

[1] Већина држава карактерише умрежене ICT, као и независне мреже, које се базирају на ICT компонентама својих националних критичних инфраструктура [28].

[2] Информационо друштво је термин, који означава скуп утицаја и друштвених последица нових ICT. Односи се на друштва у којима су комуникација, квалитет живота, економски, као и друштвени односи, посредовани технолошким артефактима (у облику производа и услуге), а који инкорпорирају научна знања [31].

[3] Неке државе су сајбер простор прогласиле, поред копна, мора, ваздуха и свемира, равноправним, петим подручјем извођења војних дејстава [26].

сајбер простора[4] је **интернет**, иницијално развијен за војне потребе и креиран крајем 60.-тих година 20. века, кроз различите пројекте Министарства одбране USA, као што је војни пројекат ARPANET. Укључивање цивилне научноистраживачке заједнице водећих америчких универзитета и института (*Stanford*, UCLA[5], *Berkeley*, MIT[6], итд.) кроз научноистраживачку Агенцију за напредне истраживачке пројекте (*Advanced Research Projects Agency* – ARPA)[7], осим стратешког, имао је и велики научно-индустријски значај [37].

Постоје различите **дефиниције сајбер**[8] **простора**, као нпр. ″глобалног подручја у оквиру информационог окружења, које је сачињено од међузависне мреже инфраструктуре информационих технологија, укључујући интернет, телекомуникационе мреже, рачунарске системе и уграђене процесоре и контролоре″ [38], или, ″сајбер простор подразумева ″врсту заједнице″ сачињене од мреже рачунара у којој се елементи традиционалног друштва налазе у облику бајтова и битова, односно, простор који креирају компјутерске мреже″ [39]. Дакле, сајбер простор је дело човека, створено применом ICT у електромагнетном окружењу у коме се подаци стварају, чувају, шаљу, примају, обрађују и уништавају, а чији су елементи подаци, системи, процеси и људи који су умрежени, или могу бити умрежени [26].

Настао као резултат техничких иновација (применом рачунарских наука и ICT) и друштвених потреба, сајбер простор јесте простор[9] креиран од друштвених мрежа [41], кога карактеришу непрекидне интеракције, односно стално/повремено умрежавање рачунарских информационих система, и чији су елементи подаци/информације, информациони системи, тј. мреже, инфраструктура ICT, сервиси, процеси и људи (аутори, корисници или учесници) [26].

Сајбер простор **није** синоним за **интернет**, већ је део ширег информационог простора, кога карактерише употреба рачунарских уређаја, софтвера и сервиса [34]. Интензиван технолошки развој и употреба иновативних технологија за бежично умрежавање, омогућило је настајање повремених (засебних) мрежа (локалних или

---

[4] О значењу појмова сајбер, сајбер простор и сајбер ратовање, затим, пореклу и еволуцији значења синтагме сајбер простор, као и дефинисању сајбер простора детаљно је дато и анализирано у [26].

[5] UCLA – *University of California, Los Angeles*.

[6] MIT – *Massachusetts Institute of Technology*.

[7]ARPA, касније DARPA (*Defense Advanced Research Projects Agency*), коју је основала Влада USA (1958), планира, води и финансира научноистраживачке пројекте из области техничко/технолошких наука за војне потребе. Настала је као одговор на претње хладног рата са Совјетским Савезом, односно као одговор на успешан развој и примену космичке технологије Совјетског Савеза, као што је успешно лансирање првог вештачког сателита Спутњик у Земљину орбиту (1957). Данас, претежно кроз нове научноистраживачке пројекте агенције DARPA, Влада USA континуирано ради на остваривању свог иницијалног циља, а то је остваривање машинске интелигенције, тј. интегрисаног плана промоције развоја и производње софтвера вештачке интелигенције.

[8] У српском језику (и другим словенским језицима, као и немачком), поред морфеме ″сајбер″ користи се и реч ″кибер″, али је употреба прве универзалнија.

[9] Сајбер простор нема физичке/видљиве границе, аморфног је облика, и има тендецију повећања, како се повећава употреба и домет информационих технологија.

глобалних), физички изолованих од интернета[10], а чија је основна сврха умрежавање у циљу остваривања специфичне функције/намене[11]. На овај начин, *ad hok* умрежавањем, али и проширивањем фиксних бежичних информационих мрежа, омогућава се да особе, објекти/ствари буду непрекидно умрежени на неку од мрежа, без повезивања на интернет.

Јединствену архитектуру **сајбер простора** сачињавају **три примарна слоја** [42, 43], који су састављени од следећих компонената (сл. 1):

- **Физички слој** – основни хардвер и инфраструктура, која омогућава генерисање, пренос и складиштење електромагнетних сигнала. Дакле, обухвата две компоненте: (а) географску компоненту[12] – физичка локација елемената мреже и (б) физичке компоненте мреже – хардвер и инфраструктуру (жичану, бежичну и оптичку), која подржава мрежу и физичке конекторе, као што су жице, каблови, радио фреквенција, рутери, сервери и рачунари.
- **Логички** (синтаксички) – сачињавају га правила, кодови и протоколи, који омогућавају добијање, манипулисање и транспорт података. Дакле, логички слој садржи логичку компоненту мреже, која је техничке природе и састоји се од логичких веза које постоје између чворова мреже[13] [44].
- **Друштвени** (семантички) – омогућава трансформацију података у смислене информације, које се преносе брзо и ефикасно, без обзира на географску удаљеност, а подржавају људске активности/циљеве (нпр. малопродаја, комуникација, итд.). Дакле, друштвени слој обухвата људске и когнитивне аспекте, и укључује: (а) компоненту сајбер личности (сајбер-персона) – *online* идентитет, тј. личну идентификацију или особу на мрежи (адреса е-поште, IP адреса рачунара, број мобилног телефона, итд.) и (б) компоненту личности – људи који су реално на мрежи; индивидуа/појединац може имати више сајбер личности (нпр. различите налоге е-поште на различитим рачунарима), а једна сајбер личност може имати више корисника [44].

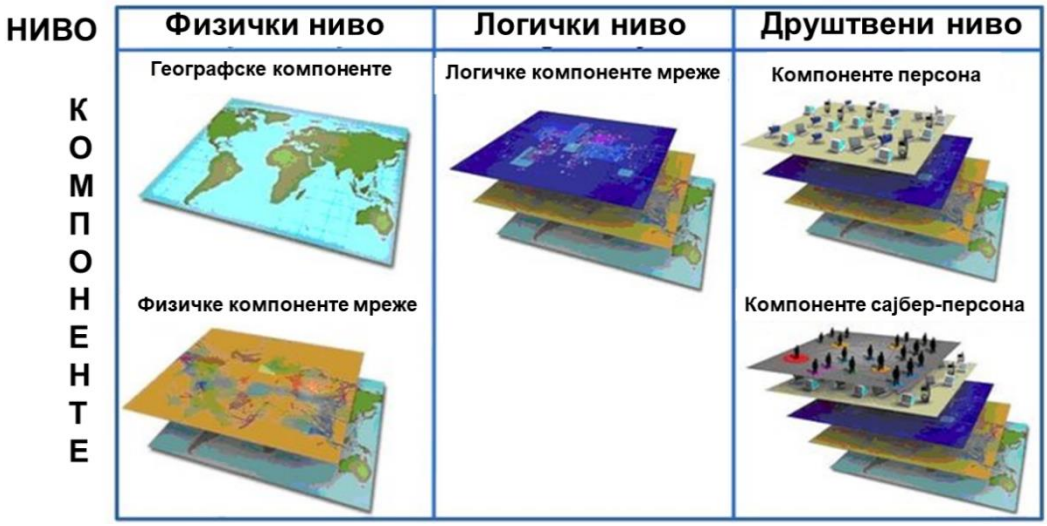
---

[10] Број засебних рачунарских информационих мрежа, које су у надлежности одређених система критичне инфраструктуре или компанијских мрежа затвореног типа, може бити веома велики (нпр. постоји око 15.000 ових мрежа, које су у надлежности Министарства одбране USA [40]. Иако се простиру глобално. попут интернета, ове засебне рачунарске информационе мреже нису предвиђене да било када буду конектоване на интернет.

[11] На пример, најфреквентније коришћени су протоколи за *ad hok* умрежавање лица (*Personal Ad Hoc Network* – PANET), возила (*Vehicular Ad Hoc Network* – VENET) или мобилних система (*Mobile Ad Hoc Networks* – MANET), затим, технологије за идентификацију и аутентификацију на малом растојању (нпр. *Radio Frequency Identification* – RFID), *Near Field Communication* – NFC или *Quick Response Code* – QR Code), као и шири концепти засновани на више различитих технологија, као што су интернет ствари (*Internet of Things*, IoT).

[12] Док се геополитичке границе могу једноставно превазићи у сајбер простору брзином приближно једнаком брзини светлости (3×10^8 ms^{-1}), још увек постоји физички аспект у вези с другим доменима сајбер простора.

[13] Чворови су сви уређаји (рачунари, мобилни телефони, итд.) повезани на рачунарску мрежу; на мрежи интернет протокола (IP), чвор је сваки уређај, који има IP адресу.



Слика 1. Слојеви и компоненте слојева сајбер простора (преузето и модификовано из [45])

Сва три слоја сајбер простора су међузависна, и оно што их повезује су подаци[14]. **Подаци** имају нумеричку вредност (представљају информацију); за остваривање интеракције с физичким окружењем, подаци се преводе у сигнале, и обрнуто. **Сигнали** се класификују на различите начине, а према особини (кардиналности) скупа вредности, које сигнал може имати, сигнали могу бити аналогни (континуални), дигитални (дискретни) и квантни.

Аналогни сигнали[15] могу имати произвољне вредности из неког опсега вредности у произвољном тренутку. Дакле, домен (време) и кодомен (вредност сигнала) математичке функције која представља аналогни сигнал су континуални скупови. Аналогни сигнал, представља се таласном (синусоидном) функцијом (зависност вредности сигнала од времена), и карактерише га минимална/максимална вредност и опсег сигнала, као и средња и ефективна вредност, односно амплитуда, период, фреквенција и кружна фреквенција. За разлику од аналогних, **дигитални сигнали** могу се представити као низ дискретних вредности, тј. у одређеном тренутку могу имати једну вредност из коначног скупа вредности. Дигитални сигнали[16] представљају информације у

[14] Сигнали представљају мерљиве физичке величине, у којима је садржана информација о неком променљивом физичком процесу. У математичком смислу, сигнал је функција, која садржи информације о одређеној физичкој појави; нпр., звук је функција притиска који зависи од координата простора и времена. У електроници, сигнал представља промену јачине електромагнетног поља, напона или струје с временом, која садржи неку информацију. Према томе, сигнал се може представити функцијом чији је аргумент време.
[15] Сви сигнали у природи су аналогни. На овим сигналима, заснива се људско опажање света (вид, звук, мирис, укус, додир).
[16] Рачунари, оптички и други електронски уређаји, заснивају се на обради дигиталних података и сигнала. За добијање дигиталних сигнала примењују се промене напона електричног импулса или прекидање напона, присуство или одсуство намагнетисаности мале области магнетног медијума, промена вредности радио сигнала, и сл.

нивоима (дискретним опсезима аналогних вредности); све вредности сигнала у једном нивоу представљају исто информационо стање.

Информација представљена једним нивоом, назива се симбол. **Дигитални сигнали** често настају семплованьем (узорковањем) аналогних сигнала, помоћу аналогно-дигиталног (A/D) конвертора, који очитава вредност сигнала у константним периодима, а добијени дигитални сигнал има дискретну (квантовану) амплитуду и представљен је у дискретним временским интервалима. У већини дигиталних кола, сигнал може имати две могуће дозвољене вредности, тј. два нивоа, и тада се назива бинарни (логички) сигнал. Представљен је са два напонска нивоа, једним, чија је вредност блиска референтној вредности, и другим, чија је вредност приближно једнака напону напајања; ови напонски нивои одговарају вредностима 0 и 1, или „нетачно“ и „тачно“; представља једноставно кодирање, тј. униполарни NRZ-L (*non-return-to-zero level*) kôd[17]. **Бинарни сигнал** у било ком тренутку представља једну бинарну цифру – ***bit*** (***Bi****nary digi****t***), и преноси најмању количину информација (симбол, тј. 1 *bit*). Због квантизације сигнала, релативно мале промене аналогног сигнала не утичу на вредност дигиталног сигнала. Најмања група битова (низ од 8 *bit*-ова) представља ***bajt*** (B).

У квантном рачунарству, користе се **квантни рачунари**, који се базирају на принципима квантне физике и за добијање сигнала користе **кубите**[18] (*qubits*), тј. квантне битове, који су направљени од квантних честица (електрона, фотона) или јона. При томе, квантни рачунари користе најважнију особину ових честица, а то је квантна суперпозиција, тј. могућност квантних честица да истовремено постоје у више дискретних стања. Ови рачунари будућности[19] омогући ће енормно брже прорачуне, тј. решавање алгоритама за оптимизацију (нпр. моделовање урагана и разбијање криптографских кључева који штите, тј. чувају приступ најосетљивијим подацима), што ће довести до великог напретка у областима климатских промена, медицине, фармакологије, финансија, логистике, итд. [46]. Ипак, сматра се да ће рачунари будућности бити комбинација класичног и квантног рачунара. Тако, предности квантних рачунара, у односу на класичне, су у решавању алгоритма за оптимизацију и брзу идентификацију најбољег решења између понуђених опција, али су инфериорнији од класичних, за коришћење *Office* алата, тј. за основне аритметичке прорачуне или извршавање команди.

---

[17] Осим NRZ-L, при преносу и складиштењу дигиталних података, користе се и други кодови, као нпр. NRZ – M (*non-return-to-zero mark*) или *Biphase* – L (*Manchester kôd*), итд.

[18] За креирање градивних елемената квантних рачунара, тј. кубита, користе се квантни процесори, и то, суперпроводљиви (суперпроводљиви кубити направљени од електрона), које развијају *IBM* и *Google*, затим, "хватачи" јона (кубити се чувају у низу јона заробљених у електричним пољима, и затим контролишу ласерима), које користе компаније *Honeywell* и *IonQ*, као и процесори базирани на светлосним квантима/честицама, фотонима. Кубити се могу креирати и од хладних атома и дијаманта (приступ који користи компанија *Intel*).

[19] Квантни рачунари захтевају коришћење ултра јаких вакуумских комора, криогенску контролу и друге инструменте за изоловање и контролу изизетних особина квантних честица, а што се искључиво може обезбедити у лабораторијским условима, тако да ће комерцијални квантни рачунари бити доступни једино кроз *cloud*. За сада, квантни рачунари су веома осетљиви – повишене температуре, електромагнетна поља и судари с молекулима ваздуха, доводе до декохеренције, тј. губитка квантних својстава кубита.

2.1.1.2. Сајбер напад

Поред великог броја корисника, у **сајбер простору** се одигравају различите **активности** (офанзивне и дефанзивне), као што су манипулација потенцијалним одлукама противника, системима и мрежама, онемогућавање приступа одређеном информационом медијуму (нпр. бежичној приступној тачки), стварање сајбер-персона, односно *online* идентитета, који олакшава комуникацију, одлучивање и утицај на јавност у когнитивној димензији сајбер простора, итд.

Могућности примене ICT, основа су за сукобе у сајбер простору, тј. извођење сајбер напада, сајбер ратовања, сајбер агресије, сајбер тероризма и сл. [34, 47]. **Сајбер напад**, генерално, представља акт агресије једног субјекта/ентитета на информациони систем другог ентитета, који се одвија у/кроз сајбер простор. Постоје различите дефиниције сајбер напада (војна, политичко-безбедносна, техничка, правна, итд.); природа сајбер напада је комплексна и вишеслојна, зависи од бројних фактора и у вези је са нарушавањем информационе безбедности. Такође, на вероватноћу сајбер напада утиче и степен развијености државе/институције/организације, а развијеније су чешће мета ових напада, с обзиром на то да су у већем уделу зависне од рачунарских система, а које покрећу/контролишу критичне националне инфраструктуре, као што је ваздушни и железнички саобраћај, систем напајања електричном енергијом, банкарство, итд.

У војном погледу, напади на информационе структуре (офанзивна дејства, обавештајне акције или операције борбене подршке), могу имати велики утицај на способност војних јединица, и то нарочито у току конфликта . Потенцијални сајбер сукоби су све реалнији, како расте зависност друштва од рањивих технологија [48]. У разматрању проблема, сматра се неопходним направити разлику између сајбер напада (различити облици ових напада) и сајбер рата[20] [49, 50]. **Сајбер рат** подразумева сајбер напад предузет од стране неког субјекта међународног права с намером да почини акт агресије над другим субјектом међународног права, и подлеже принципима и нормама Међународног права оружаних сукоба. Ипак, број сајбер ратова, много је мањи од броја сајбер напада, који се односе на сајбер криминал, тј. ситуације у којима је прекршен кривични закон неке државе или међународни прописи кривичног права [49]. Међутим, чињеница је да је сајбер рат највећи безбедносни изазов 21. века [51], као и да су најразвијеније државе најрањивије у сајбер простору. Свакако, савремене војске се проактивно баве свим аспектима сајбер ратовања, као и супростављањем претњи од сајбер ратовања.

У техничком смислу, **сајбер напад** ″представља намерно угрожавање информационе безбедности неког система или информација садржаних у њему, предузето од стране неког ентитета, заобилажењем безбедносних механизама система, злоупотребом недостатака у систему техничке и нетехничке природе″ [26]. Директни циљ ових напада јесте нарушавање информационе безбедности, а

[20] Према Младеновићу и аут. [49], сајбер ратовање представља ″офанзивну и дефанзивну примену сајбер оружја и информација, коју су покренули и организовали државни актери ради уништавања или онеспособљавања противничког циља директним дејством на информације и информационе системе и посредним дејством на системе, средства, сервисе, процесе, друштво и појединце који зависе од тих информационих инфраструктура, као и одбране властитих ресурса од таквих дејстава противника″.

индиректни циљеви су откривање података/информација и уништавање, оштећење или онеспособљавање информационих система, као и лица и система који зависе од примарно нападнутог система. Генерално, сваки сајбер терористички напад проузрокује индиректне ефекте, које нападачи теже да остваре, а то су ефекти напада на системе/уређаје који су под контролом рачунара–мете, као и на доношење људских одлука.

У сајбер простору, глобално умрежавање, тј. успостављање глобалне мреже међусобно повезаних корисника, дакле, интернет и друштвене мреже, омогућило је настанак новог, савременог облика тероризма – **сајбер тероризма**, а с обзиром на то да ово умрежавање омогућава географски неограничене и брзе активности/акције [34, 52].

С друге стране, технолошки развој омогућио је и стварање глобалне мреже међусобно повезаних објеката (ствари) – **интернета ствари**[21] или интернета интелигентних уређаја (*Internet of Things*, IoT) [29, 41, 47, 55–58]; ови објекти (технологије, уређаји и алати) конектовани преко јавне или приватне мреже интернет протокола (IP), користе се заједно у интернет апликацијама у циљу размене података с произвођачем, оператером и/или другим повезаним уређајима, са било ког места, у било које време. Дакле, то је скуп међусобно повезаних уређаја (систем механичких и дигиталних машина и предмета), који омогућавају преношење података путем интернета, без интеракције између људи, или људи и рачунара – **IoT** су физички објекти/ствари с уграђеним сензорима[22], софтвером и другим технологијама, које им омогућавају да преносе и примају податке у оба смера (ка, и од других ствари и система), у циљу информисања корисника или аутоматизације радње[23]. Тако, уређаји добијају тзв. дигиталну интелигенцију – уређаји без учешћа човека користе потребне податке у одређено/одговарајуће време, помоћу којих могу сами регулисати свој рад. То могу бити веома једноставне ствари, али и много сложеније, као нпр. млазни мотори опремљени хиљадама сензора за прикупљање података и слање повратних информација. Шта више, целе регије/области могу бити опремљене сензорима, у циљу контроле животне средине (за мерење нивоа буке и загађења) или вршење безбедног надзора над тим подручјима. Осим стандардне конекције, углавном преко Wi-Fi мреже, већина IoT

[21] Термин *Internet of Things* увео је 1999. год. *Kevin Ashton* (креатор глобалног стандардног система за *Radio Frequency Identification* (RFID) и друге сензоре, и кооснивач *Auto-ID Center*, MIT), да би описао систем у коме је интернет повезан са физичким светом преко свеприсутних сензора [53].

[22] Сензори на интернету представљају уређаје, који су технолошки пројектовани да примају и шаљу информације преко интернета (нпр. нови модели возила, паметни телевизори, мерачи протока саобраћаја, термометри, медицински уређаји, итд.).

[23] IoT су програмирани да прикупљају и анализирају податаке, у циљу добијања информација и аутоматизације наредних радњи/одлука. Овај процес, тј. IoT систем, састоји се из следећих компоненти: (а) прикупљање података – преко сензора, IoT уређаји (један сензор или уређај са више сензора) прикупљају податке из свог окружења; (б) повезивање/дељење података – користећи доступне мрежне везе (Wi-Fi, *Bluetooth*, итд.), IoT шаљу прикупљене податке у *cloud* (уређај–систем–уређај) или на други уређај (уређај–уређај); (в) обрада података – софтвер анализира и безбедно обрађује податке, као и предузима одређену активност (нпр. укључи вентилатор или пошаље упозорење) и (г) кориснички интерфејс – обезбеђује резултате обраде података крајњем кориснику [55, 56].

користи неки облик бежичне конекције, као нпр. *Bluetooth Low Energy* (*Ethernet*[24] – у оквиру унутрашње мреже), LTE (*Long Term Evolution*) или чак сателитске везе. У данашње време, постојање других врста мрежних платформи, као што је 5G мрежа[25], јесте обећавајући потенцијал за манипулацију с огромним скуповима података, скоро свуда, и с великом брзином и поузданошћу.

У сајбер простору, подаци се размењују између људи и људи, ствари и ствари, као и ствари и људи, преко стандардизованог ″језика комуникације″, затим, интернет везе (средство које омогућава комуникацију), као и IP (располаже адекватним капацитетом, који омогућава комуникацију између многобројних потенцијалних учесника, тј. IPv6 адресама)[26]. Тако, IoT концепт јесте парадигма света у коме се спајају дигитално, стварно и виртуелно, у циљу стварања **паметног окружења** (паметно осветљење, грејање, куће, итд.), које енергију, транспорт, градове, итд., чине интелигентнијима. Неки од важних уређаја[27] и повезаних технологија за IoT су нпр. камере за надзор, мерачи загађености ваздуха, мерачи радиоактивности, технологије за идентификацију и аутентификацију на малом растојању (*Radio Frequency Identification*, RFID), сензорске мреже, дронови, итд. [29].

Интегрални развој IoT је повећање, како броја сензора, тј. уређаја који су технолошки пројектовани да примају и шаљу информације путем интернета, тако и њихових корисника [59] Додавања једног сензора с отвореним приступом на мрежи, енормно повећава број његових учесника/корисника, и омогућава различитим актерима (државним и недржавним) предузимање различитих малициозних активности, тј. узрокује енормни пораст могућих злонамерних упада у системе, који су осетљиви на сајбер нападе (нпр. регулаторе притиска у гасоводима, електронски контролисане вентиле у нуклеарним постројењима, медицинске уређаје, итд.). Због тога је безбедност рачунарских мрежа од посебног значаја, нарочито у критичним инфраструктурама, а рачунарска безбедност јесте изазов за очување димензије јавне безбедности [60].

Сматра се да је **сајбер простор**, осим појединцима, све више значајан државама, као подршка њиховим стратешким интересима. Сајбер простор постаје инструменат националне моћи, тј. потенцијално средство принуде [61, 62]. У том контексту, више од 2/3 сајбер инцидената укључивали су актере у азијско-

---

[24] *Ethernet* (етернет) је локална мрежа (LAN), која повезује уређаје на малој географској локацији, за разлику од интернета, који представља мрежу широког подручја (VAN).

[25] 5G мрежа омогућава нпр. повезивање милиона уређаја, који подржавају ову мрежу, на једном km^2. То ће омогућити коришћење великог броја сензора у веома малом простору, и тако повећати употребу, као и ефикасност IoT технологије [57, 58].

[26] Интернет је глобална мрежа која се састоји од *Transmission Control Protocol* (TCP) у комбинацији с различитим протоколима, као што су IPv4 и IPv6. IoT уређаји најчешће немају подршку за ове протоколе, што онемогућава директну везу с њима (или са њих). Комбинација IPv6 (тренутни интернет протокол) и бежичних мрежа мале снаге (нпр. 6LowPan), омогућава IoT уређајима директни приступ TCP/IP Интернету. То значи да чак и најмањи и најслабији IoT уређаји могу имати могућност повезивања.

[27] Термин IoT користи се најчешће за уређаје који могу да остваре комуникацију с мрежом, независно од људског учешћа. У том смислу, рачунари се генерално не сматрају IoT уређајем, као ни паметни телефони (иако су то уређаји с бројним сензорима).

пацифичком региону, а различите сајбер активности (од покушаја шпијунаже до принуде), као и растуће тензије у овом региону, у први план стављају неопходност бољег разумевања стратешког коришћење сајбер простора [62]

Суштина постојања сајбер напада је искоришћење недостатака/грешака, тј. **рањивости** (део 2.1.2.) у техничким (хардвер), софтверским и информационим системима. С друге стране, системи који немају рањивости/слабости, отпорни су на сајбер нападе. Због тога, вероватнији нападач у сајбер простору јесте особа којој су познате рањивости неког система, и која има знање да их ефективно искористи, него актер с искључиво непријатељским намерама. **Нападач** у сајбер простору је особа која користи своја знања из области ICT у циљу угрожавања безбедности рачунарских система, а било која акција која ову безбедност угрожава, представља **напад**.

Актери нападе могу бити особе, корисници система или они изван система. Нападачи се могу класификовати (у погледу безбедности рачунара) на: *White Hat* хакере (тзв. хакери са белим шеширом) – добронамаерни хакери, који користе исте технике и алате као и потенцијални злонамерни хакери (нападачи), али за разлику од њих, не оштећују систем и не краду информације, већ детектују безбедносне пропусте система, и о томе извештавају власника, као и о начинима уклањања грешака и пропуста; *Black Hat* хакере (тзв. хакери са црним шеширом), крекери (*crackers*) – злонамерни хакери, тј. они који нарушавају безбедност система, без одобрења. Често су креатори злонамерних програма, тј. компјутерских вируса, црва, тројанаца, у циљу крађе података и оштећења компјутерских система; *Grey Hat* хакере (тзв. хакери са сивим шеширом) – неморални хакери, који најчешће немају злу намеру, али понекат предузимају незаконите активности у циљу испитивања и надгледања система у које су продрли; *Blue Hat* хакере (тзв. хакери са плавим шеширом) – хакери које унајмљују велике компаније у циљу проналажења и решавања безбедносних пропуста (нпр. компанија *Microsoft*, која у сарадњи са *Blue Hat* хакерима ради на побољшању безбедности својих производа).

Дакле, за остваривање сајбер напада, неопходно је спајање рањивости система и техничке способности нападача за извођење прикривених нападачких активности.

2.1.2. Рањивости као кључни чиниоци сајбер напада

Сваки систем, па тако и компјутерски има одређене рањивости, а то, из угла безбедности, представља његов негативан аспект. Сваки недостатак у рачунарском систему/делу рачунарског система, као нпр. грешке у софтверу, његовој имплементацији, функционисању и интеракцији, повећавају вероватноћу остваривања потенцијалних **претњи** (*threats*). **Рањивости** (*vulnerabilities*) су тачке слабости у систему, тј. грешке у рачунарским апликацијама, слабости корисника и све оно што може довести до угрожавања поверљивости, интегритета или доступности података [63].

Методе сајбер напада нису универзалне, а сваки сајбер напад, зависнији је, у техничком смислу, од циља/мете, тј. њене рањивости, него од нападача [26]. **Рањивости** подразумевају недостатке/слабости/неусклађености елемената или

компонената сајбер простора, а произилазе из међусобно зависних интеракција основних компоненти сајбер простора, што повећава могућности за постојање недостатака, како у дизајну, тако и функционисању. Осим софтверских грешака (логички ниво сајбер простора) и хардверских недостатака (физички ниво сајбер простора), и сви други фактори (интерни, екстерни и функционални), који омогућавају функционисање и употребу система, на сваком од три нивоа сајбер простора (физички, логични и друштвени, сл. 1), омогућавају широк спектар активности, које могу довести до угрожавања информационе безбедности, тј. до сајбер напада [64]. Рањивости, осим информационе природе, могу бити и техничке, друштвене, организационе, правне, итд., а сајбер напад, односи се искључиво на агресивне активности, које користе информациони систем, и чији су примарни циљеви ови системи [65, 66].

Упркос напорима да се сајбер простор заштити од претњи његовој поверљивости, интегритету и доступности, сматра се да је константно изложен различитим опасностима. Као што је поменуто, комплекснији систем је потенцијално рањивији на сајбер нападе, јер функционисање оваквих система захтева специјализована знања о дизајну, имплементацији, раду и управљању [62, 67].

Грешке у софтверу, као и сензорском и мрежном хардверу, могу довести до **отказа у раду система**, и тако имати катастрофалне последице. У сајбер простору, кључно место напада јесте његов логички слој, тј. **софтвер**[28], који повезује овај слој са преостала два, физичким (инфраструктура, мрежни и преносни уређаји, тј. хардвер) и когнитивним слојем (информације настале као резултат интеракције физичког и логичког слоја, тј. инструкција за обраду података и креирање информација, које подржавају различите људске активности).

Једно од основних својстава софтвера је **безбедност** (поверљивост, интегритет, непорецивост, аутентичност и одговорност), која представља ″ниво до кога производ или систем штити информације и податке тако да особе или други производи или системи имају ниво приступа подацима који одговара врсти и нивоу њихових овлашћења″ [68]. Квалитет софтвера, свих његових карактеристика (функционална подобност, ефикасност учинка, компатибилност, употребљивост, поузданост, безбедност, могућност одржавања и портабилност), као и подкарактеристика, зависе од специфичног контекста употребе [68]. **Грешке у програмирању**, тј. софтверу (број и доступност), утичу на могућност предузимања сајбер напада, тако да представљају рањивости датог информационог система, независно од њиховог значаја, или од тога да ли се користе у војне или цивилне сврхе. Ове грешке су неизбежне, с обзиром на то да су у директној вези с природним ограничењима људског рада. При томе, вероватноћа настајања грешке/недостатка, одређена је сложеношћу (величином) софтвера, тј. бројем његових кодних линија[29], без обзира на степен сложеност кодних логичких инструкција – већи број кодних

[28] Софтвер је интегрални део сваког информационог система.

[29] Кодна линија софтвера јесте обим/број логичких исказа/процеса и различита је за различите софтвере, односно различите врсте програмских језика. Користи се за процену очекиваног уложеног рада програмера за програмирање неког софтвера, као и одржавање/продуктивности процеса израде софтвера.

линија узрокује већу вероватноћу настајања недостатака. Затим, рањивости представљају и конективност, као и надоградљивост софтвера, особине својствене ICT, а које се креирају у циљу компатибилности, тј. функционалности; свако додатно побољшање квалитета програмирања веома је скупо, јер подразумева дуготрајно тестирање софтвера у различитим ситуацијама [69]. Међутим, у неким институцијама, као што је *National Aeronautics and Space Administration* (NASA), програмирају се софтвери изузетног квалитета.

Грешке у **софтверу**[30] могу имати различите последице на функционалност одређеног система, од смањена функционалности (као нпр. у *web*-окружењу) до тренутног отказа функционалности у системима високог ризика (нпр. **ваздухопловни,** војни и нуклеарни системи), а што може имати потенцијално трагичне последице на посаду/људе/околину, као и довести до угрожавања националне безбедности. С друге стране, веома је тешко утврдити узроке софтверских грешака, тј. да ли су случајне (постоје у програму, али се испољавају у специфичним ситуацијама, условљене окружењем и спољашњим факторима), или су намерно изазване (нарочито у случају отказа/уништења система). Сајбер напади тешко се детектују, нарочито уколико се реализују злоупотребом недостатка, који се инкорпорирају у информациони систем, тако да жртва нема свест о извршеном/постојању напада. Грешке се спречавају тестирањима софтвера, што може бити веома захтевно и скупо (као код високоризичних система) или знатно брже и јефтиније (окружење *veb* презентација и апликација).

За **примену/детекцију сајбер напада**, много је значајније познавање **слабости/рањивости** неког система и поседовање капацитета за продор у систем, него намера нападача да предузме непријатељске активности. Нарочито, у случају информационих система, који су физички изоловани од доступних мрежа/других система, као што су војни системи, откривање рањивости и продор у систем, тј. остваривање сајбер напада од стране појединца, изузетно је захтевно. С друге стране, тимови државних агенција специјализовани за извођење офанзивних активности у сајбер простору, као нпр. *Tailored Access Operations* (TAO)[31], у саставу *National Security Agency* (NSA), поседују неупоредиво веће ресурсе од појединаца/групе, у сваком смислу – располаже већим новчаним средствима и информацијама о већем броју **рањивости нултог дана** (*zero-day, 0-day vulnerabilites*)[32], као и окупља већи број експерата [65] и нарочито, има конкуренску

[30] Грешке се могу класификовати на: (а) квар/грешка (*bug*) - грешка општег карактера [70] (б) недостатак/мана (*flaw*) – грешка у додељивању/недодељивању/надзору, а што омогућава заобилажење/онемогућавање заштитних механизама [71], (в) отказ (*failure*) – привремени/стални прекид способности неког ентитета да извршава захтевану функцију [72] и (г) квар (*fault*) – абнормално стање/дефект компоненте/опреме/подсистема, а које може довести до отказа [73].

[31] TAO је NSA Одељење за операције рачунарске мреже, која идентификује, надгледа, инфилтрира се и прикупља обавештајне податке о компјутерским системима, а које користе ентитети ван USA [74].

[32] Ове рањивости односе се на рањивости у софтверу, које нису познате произвођачима, нити јавно, тј. познате су нула дана. За ове рањивости се не прави безбедносно ажурирање (поправка) система, тако да, уколико их открију малициозни хакери, представљају велики ризик за кориснике информационог система. Дакле, напад нултог дана дешава се када малициозни хакери искористе грешку, пре него што програмери исту отклоне [75].

предност, према изјавама актуелног директора ТАО, Роба Џојса [76]. При свему овоме, веома је важно разумети захтеве држава да успоставе ефикасан војни сајбер капацитет, уз претпоставку да државни актери углавном спроводе циљане сајбер операције стратешког значаја, а не опортунистичке, које немају стратешку сврху [77].

Дугачка је листа софтверских грешака, које су евидентиране, како у војним борбеним системима, тако и у цивилним (нпр. цивилној авијацији), и представљају веома озбиљне ризике по информациону безбедност техничких и организационих система [78].

С аспекта безбедности, рачунарски системи могу бити угрожени различитим врстама напада, или њиховом комбинацијом [79]. У наставку ће бити укратко описани карактеристични напади (претње), а то су: DoS (DDoS), *Spam*, *Phishing*, *Botnet*, *Sniffing*, *Spoofing* и *Malware*.

- ***Denial-of-Service***

DoS (напад ускраћивањем услуга) – У DoS нападу, преоптерећењем мрежних сервиса или прекомерном конекцијом, покушава се спречавање легитимних корисника да приступе мрежи/услугама. С обзиром на то да се инфраструктура међусобно конектованих система и мрежа састоји од ограничених ресурса, DoS алатима, шаљу се бројни захтеви циљаном серверу, најћешће *web*, *file transfer protocol*, *e-mail* сервер, у циљу онеспособљавања сервера, тј. успоравања/потпуног престанка његовог рада. Врста овог напада, који се појавио 1999. године (шире од 2000. године, када су оборени популарни сајтови *Amazon*, CNN, *eBay*, *Yahoo*, итд.) је *Distributed Denial of Service* (DDoS), који користи снагу вишеструких посредних корисника. То су озбиљнији напади од DoS напада, у којима се користи већи број рачунара заражених рачунарским црвима или тројанцијама за реализацију скоро истовременог напада на систем–мету. DoS и DDoS нападе веома је тешко детектовати и спречити, а најбоља одбрана од истих је промена конфигурације рутера код провајдера интернет услуга.

- ***Spam*** (спем)

Спем, или нежељена електронска пошта (корисних је није тражио, као и није дао сагласност пошиљаоцу за слање истих). То су најчеће рекламне поруке/понуде, међутим, могу бити и поруке чији је циљ убацивање малициозног софтвера у рачунар – мету. Спем је облик електронске поште, који покушава да прикрије e-*mail* адресу пошиљаоца и тако онемогући његово праћење, или облик електронске поште, који се користи обмањивањем при навођењу "предмета" (*subject*) и тако натера примаоца да отвори примљену пошту. Најчешће, *e-mail* адресе се прикупљају коришћењем роботских сакупљача (*harvester*) – бота, а нападачи међусобно размењују прикупљене базе података, тј. *e-mail* адресе. Инфраструктура нападача, најчешће је у државама које немају законске оквире и дефинисане казне за ову врсту активности. Спем постаје све већи и озбиљнији проблем на интернету, што је делом узроковано природом интернета као дистрибуираног систама, а који се реално не контролише и који је развијен тако што су бројне одлуке у вези с овим системом донесене консензусом. Осим за појединачне кориснике, велике количине спем порука представљају проблем и за интернет провајдере (*Internet Service Provider,* ISP), који због тога морају да повећавају своје капацитете. За заштиту од

спема, користе се софтвери за филтрирање, али је значајна и едукација као и примена анти-спем регулатива и других мера.

- ***Phishing*** *(*фишинг*)*

Фишинг је напад у коме нападач употребљава постојеће интернет сервисе у циљу преваре, тј. откривања осетљивих информација корисника, као што су корисничка имена, лозинке, подаци с кредитних картица, итд., а које може користити у криминалне сврхе. Изводи се тако што нападач (фишер) користи лажне електронске (интернет) адресе, које личе на званичне, тј. оне које шаљу одређене институције, нпр. банке, с којима жртва има контакт. На пример, фишер пошаље *e-mail* кориснику банке у коме га обавештава о укудању рачуна, уколико не ажурира личне информације, као и линк ка лажном сајту (верна копија стварног сајта банке) коме треба да приступи. Тако, потенцијална жртва бива "упецана", тј. намамљена на лажни *web* сајт, где ће навести број свог рачуна и приступну лозинку, што се касније може злоупотребити, најчешће из финансијских мотива. Поред електронске поште, фишери користе и различите интернет сервисе (*Windows Messenger, Skype, Google Talk*), друштвене мреже (*Facebook, Twitter, MySpace*), итд. Као основни алат у фишинг нападу, користи се *spam* у циљу остваривања што већег броја потенцијалних жртава напада; за слање електронске поште, која ће бити веома слична легитимном захтеву, фишери користе базе података (*spamer's database*), које садрже бројне *e-mail* адресе. Фишери користе и *botnetove* у циљу остваривања истовремених покушаја бројних фишинг напада.

- ***Botnet*** *(комбинација настала од речи ро**бот** и **нет**ворк)*

Ботови (*bots,* скраћеница од *ro**bots***) – рачунарски програми (најчешће извршни фајлови) инсталирани на рачунар у циљу аутоматског покретања сета функција, који омогућавају неовлашћеним корисницима аутоматску контролу преко комуникационог канала. Ови ″заражени″ рачунари називају се зомбији (*zombies*) или ботови (*bots*), и могу се налазити било где у свету. Ботови су увек део координиране бројне групе заражених (истим малициозним програмом) персоналних рачунара (или мобилних телефона новије генерације, *smartphones*), на којима су инсталирана ″zadnja vrata″ (*backdoor*) за извршавање команди. Ботови, даљински контролисани, шаљу *spem*-ове, дистрибуирају оглашавачке програме (*Adware*), предузимају DoS нападе, итд., у циљу крађе идентитета, шпијунаже, али и напада на критичне информационе структуре (нпр. DDoS напад на финансијске и институције Владе Естоније (мај, 2007) изведен је коришћењем 560 рачунарских мрежа из преко 50 држава [63].

- ***Snifing*** (снифери)

Снифери су хардверски и софтверски алати, којима се може пратити мрежни саобраћај и тако прикупљати подаци (законито или незаконито). Њушкање (*sniffing*) се једноставно реализује на тзв. сегментираној, тј. подељеној мрежи (*shared network*). Нападач, који има физички приступ мрежи, може на исту поставити ″сниферски алат″, тзв. анализатор протокола (*protocol analyzer*) и пратити сва дешавања на одређеном сегменту мреже. Тако, рутер са снифером, може читати податке у оквиру пакета, као и изворишну и дестинациону адресу. Снифери се међусобно разликују према функционалности и дизајну, а познатији су *Ethereal, Tcpdump*, итд.

- ***Spoofing*** (спуфинг)

Спуфинг је техника у којој се провера аутентичности, у тренутку конекције, једне машине према другој, изводи фалсификовањем пакета из IP адресе извора коме се верује. Најједноставнија врста спуфинга је IP спуфинг, у коме се фалсификује изворна адреса IP пакета (IP адреса и многобројна поља IP заглавља), али постоје и друге технике спуфинга, као што су *Address Resolution Protocol* (ARP) спуфинг (фалсификовање *Media Access Control,* MAC адресе Етернет (*Ethernet*) фрејмова и *Domain Name System* (DNS) спуфинг (фалсификовање података у DNS пакетима).

- ***Malware*** (малвер)[33]

Малициозни софтвери који могу нанети веома велику штету зараженом рачунару – мети. Једноставно се шире интернетом и могу бити различите природе (јачине малициозне активности, начина умножавања и извршења).

Рачунарски вирус – малициозни програми, који се шире самореплицирањем, тј. убацивањем својих копија у други извршни кôд/документ, тако инфицирајући датотеке и програме на рачунару – мети. Наносе штету зараженом рачунару, тј. софтверу, бришући или мењајући фајлове на диску рачунара. Рачунарски вируси се једноставно преносе, преузимањем заражених фајлова са интернета/другог умреженог рачунара или преко преносног диска. Постоје различите врсте рачунарских вируса, као што су полиморфни (мењају облик да не би били детектовани), затим, невидљиви (прикривају присуство од апликација), као и ретро вируси (нападају/заобилазе антивирусне програме), итд. Међутим, рачунарски вируси нису програмирани за ширење преко рачунарских мрежа, тако да су данас изгубили на актуелности. За разлику од рачунарских црва, за ширење рачунарских вируса, потребан је *host* програм.

Рачунарски црв (*worm*) – врста малициозног софтвера, који се вишеструко умножава преко рачунарских мрежа. За разлику од рачунарског вируса, рачунарски црв је самостални програм, који се не качи за главне извршне програме, а преноси се на друге системе аутоматски (без људске интервенције), преузимањем контроле над рачунарским функцијама тако предузимајући малициозне активности (брисање фајлова, слање података без знања корисника, итд.).

Тројански коњ (*trojan horse*) – злонамерни програм, који се прерушава у легитимни програм (најчешће забавни, као нпр. игрица), у циљу крађе информација и заузимање простора на диску рачунара, меморији итд. За разлику од рачунарског вируса, не може се самостално умножавати, већ га преноси корисник, његовим копирањем на други рачунар. Постоје различите врсте тројанаца, као што су тројанци за даљински приступ, за откривање и давање лозинки, *Keyloggers,* FTP тројанци, и др.

Шпијунски програми (*spyware*) – малициозни програми, који прикупљају персоналне информације, податке о коришћењу рачунара, као и посети одређених сајтова.

Rootkit – један, или више програма, тако дизајнираних да не може открити угроженост рачунарског система – мете, а имају за циљ преузимања контроле над

[33] *Malware* – сложеница од енглеских речи ***mal****icious* и *soft****ware****.*

рачунарским системом, као и избегавање откривања присуства при скенирању антивирусних програма. Различите варијанте *rootkita* су у оптицају, као легалне апликације, тројански коњи, итд. Детекција *rootkit* програма врши се *cross-view* техником, као и методама заснованим на провери интегритета података и меморије. Како се константно појављују нови *rootkit* програми, неопходно је користити већи број комерцијалних алата (*UnHackMe, Proces Master*, итд.), као и алата отвореног кода (*Sophos Anti-Rootkit, RootKit Hook Analyzer*, итд).

Оглашавачки програми (*adware*) – малициозни програми инсталирани на рачунар – мету, без знања његовог корисника. При претраживању на інтернету, ови програми приказују огласе (*advertisements*).

Успоравање рада рачунара, појављивање нових датотека, неправилни рад апликација (*web* претраживачких, програми за обраду текста), итд., су само неки од показатеља присуства малициозног програма у рачунару – мети.

Као што се и претпостављало [80], активности у сајбер простору, охрабриле су државне актере да користе сајбер напад као инструмент принуде. У том смислу, **најпознатије** операције у **сајбер простору** су **естонски DDoS** (2007) и **ирански Стакснет** (*Stuxnet*) (2010) сајбер напади, а који потврђују потенцијале извођења операција у сајбер простору.

Широки DDoS напад (2007) на естонске Владине и финансијске институције у сајбер простору (трајао је двадесет два дана) био је резултат политичког сукоба између Естоније и Русије[34]. Ови напади ускраћивањем услуга, изазвали су привремену деградацију/губитак услуга на бројним комерцијалним и државним серверима. Већина напада била је усмерена на некритичне услуге (јавне *web* сајтове и е-пошту), док су други били концентрисани на виталније циљеве, као што је *on-line* банкарство и DNS [64]. Након тога, као резултат стратешког партнерства *Europe Union* (EU) и *North Atlantic Treaty Organization* (NATO) у области одбране (укључујући и сајбер одбрану), у Естонији је успостављен (2008) Кооперативни центар изузетности за сајбер одбрану (*Cooperative Cyber Defence Centre of Excellence,* CCDCOE), у циљу обуке, истраживања и развоја у области сајбер одбране.

Најпознатија сајбер операција Стакснет (*Stuxnet*), предузета је против иранског програма развоја нуклеарног наоружања, тј. остварена коришћењем више малициозних компјутерских програма, којима су нападнути информациони систем и уређаји нуклеарног постројења у Натанцу у Ирану (2010), а који су били потпуно одвојени од интернета [81–83]. То је први „наоружани“ малвер, који је користио шест различитих рањивости система, и који је значајно пореметио нуклеарне амбиције Ирана – програм развоја нуклеарног наоружања ове државе је онемогућен/пролонгиран за одређени период, због утицаја малвера на систем

[34] Повод за напад била је одлука естонске владе да премести споменик совјетског војника у Талину, на оближње војно гробље. Споменик је подигнут (1947) на месту где су сахрањени совјетски војници, који су погинули у заузимању Талина у Другом светском рату. Временом, споменик је симболично постао жариште напетости између локалне руске мањине, за коју је споменик представљао „ослободиоца“, док је за естонски националистички покрет, био симбол ″угњетача″.

производње нуклеарног наоружања. Ова сајбер операција била је удружена акција специјалних јединица више држава (сматра се Израела и USA) [84, 85], а најважнији корак те операције, било је добијање поверљивих информација неопходних за инфилтрацију у иранско нуклеарно постројење, као и креирање софтвера, а што је обављено у физичком окружењу, изван сајбер простора. Сматра се да, иако великог потенцијала, реална штета коју је изазвао Стакснет, није била већа од штете коју би изазвали нпр. оперативни кварови система [86, 87]. Ипак, потпуна процена изазване штете није транспарентна, јер нападнута држава свакако неће открити нападачима своје евентуалне слабости и степен успешности напада. Како било, Стакснет је први рачунарски софтвер, тј. прва јавно позната претња коришћена за критичне инфраструктуре, као што су нуклеарне електране, бране и хемијска постројења [88]. Реализација оваквог напада, како се показало, је једноставна, што указује на неизбежност вођења сајбер ратова [48].

Интерес држава, које предузимају **сајбер операције** – офанзивне или дефанзивне (одбрамбене) је активна процена ризика, као и одговорно откривање рањивости, што би ограничило њихову експлоатацију, као и смањило употребу офанзивних сајбер операција. Свакако, **сајбер напади**, који су усмерени на нелегитимне мете, тј. они који могу угрозити цивилне објекте и грађане, без изузетка су забрањени, док легитимне мете сајбер напада могу бити нпр. војни циљеви или припадници оружаних снага [89]. При томе, процена оправданости сајбер напада је питање Међународног права оружаних сукоба, али и права у општем смислу, јер је недопустиво да се предузети сајбер напад оправдава тиме што нападнута страна није успоставила, или није имала могућност/способност да успостави неопходан систем информационе безбедности својих информација и система [26].

Дакле, активношћу различитих чинилаца у сајбер простору, настају сајбер претње, које се генеришу из различитих извора; кључни извори сајбер претњи, сумарно су дати у Табели 1 [90, 91].

Важно је истаћи да постоји заједнички интерес држава које спроводе сајбер операције (одбрамбене или офанзивне), у активном процењивању ризика и бенефита од нетранспаретног приказивања рањивости у циљу експлоатације истих. С друге стране, сматра се да је, **одговорно откривање новооткривене рањивости**, у националном интересу. Уколико је тако, одговорнија детекција и ажурирање рањивости, довело би до смањења броја рањивости и њихове експлоатације, што би повећало цену развоја офанзивних способности, и стога ограничило пролиферацију, као и смањило употребу офанзивних операција.

Табела 1. Различити извори сајбер претњи [90, 91]

Извор претње	Коментар
Државе	Државне обавештајне службе, користе IT средства у циљу прикупљања информација и шпијунаже; ове активности могу бити усмерене на друге државе (у циљу дезинформисања, дестабилизације, застрашивања или вођења сајбер рата), али се могу односити и на недржавне претње (коришћењем личних података, некада без судског налога и адекватног демократског надзора, доводе до угрожавања људске безбедности); сајбер претње у организацији држава, могу се односити само на информационе системе, али не и на цивилне ентитете (болнице, школе, инфраструктурна постројења и сл.)
Корпорације	Компаније и корпорације, самостално, или у сарадњи с криминалним групама/хакерима, спроводе индустријску шпијунажу и/или саботажу (преузимање контроле над системом за обраду података); корпорације су претња, јер прикупљају и анализирају бројне личне податке, а у неким случајевима их деле с владама/другим приватним актерима
Хакери	Хакери у данашње време, не морају поседовати значајно компјутерско знање и вештине – *download*-ом (са интернета) сценарија сајбер напада и протокола, средства за напад на сајтове мета, много су једноставнији и софистициранији, у односу на раније
Хактивисти	Хактивизам је комбинација хаковања и традиционалног активизма, и даје нове могућности анктивистима на друштвеним мрежама у њиховој борби за остваривање одређеног циља (нпр. слобода говора, људска права, итд.). Хактивисти углавном користе тактике ширења рачунарских вируса и црва, DDoS, манипулације интернет страницама и сл., тако преузимајући корисничке налоге на друштвеним мрежама или прикупљати и/или откривати осетљиве и личне информације из система – мете. Иако се не сматрају деструктивним, хактивисти могу сарађивати са сајбер криминалцима, тако да је танка линија раздвајања између хактивизма и напада у сајбер простору
Фишери	Појединци/групе људи, који најчешће користе *spam* или *malware* у циљу крађе идентитета/информација, а за остваривање финансијске добити

Незадовољни појединац унутар сајбер простора (инсајдер)	Појединац који изражава своје незадовољство због личне моралне дилеме/неслагања с државном политиком, представља озбиљну претњу, јер му детаљно познавање система–жртве, омогућава неограничени приступ. Најпознатији је случај Едварда Сноудена, бившег службеника америчке Централне обавештајне агенције (CIA) и узбуњивача, који је обелоданио тајну документацију о америчким пројектима надзирања и хакерским нападима
Терористи	Особе, које имају непријатељске намере, а за организовање програма рада и неовлашћени приступ информационим системима влада и приватних ентитета, користе рачунаре као алат. Мотиви су политичке, социјалне или економске промене, и циљеви уништавање, онеспособљавање или искоришћавање кључне инфраструктуре, угрожавање националне безбедности, изазивање масовних људских жртава, нарушавање јавног морала и поверења широке јавности
Ботнет оператери	Хакери који преузимају и контролишу већи број рачунара, а које су претходно заразили вирусом; преко ових рачунара координишу сајбер нападе, фишер преваре, спамовање, малвер нападе или друга штетне активности (финансијске малверзације и крађу поверљивих података)
Аутори шпијунског и злонамерног софтвера	Организације/појединци, с злом намером, користећи и ширећи шпијунски и малициозни софтвер (*malware*) нападају рачинаре – мете
Појединци који злоупотребљавају интернет и друштвене мреже	Негативан аспект коришћења интернета (у приватном, као и пословном сектору); ова злоупотреба интернета и друштвених мрежа, обухвата узнемиравање и прогањање, злоупотребу личних података и фотографија, дељења недозвољених и штетних садржаја, сајбер *bullying* (сајбер застрашивање/насиље), итд. Забрињавајуће је низак ниво свести корисника интернета о могућим злоупотребама и последицама, као и чињеница да су могућности заштите појединца веома мале

2.2. КОНЦЕПТ САЈБЕР БЕЗБЕДНОСТИ

Суштински, сајбер безбедност у вези је са заштитом ресурса (материјалних и/или нематеријалних) од евентуалних опасности [92, 93]. Све више, питање сајбер безбедности односи се на одржавање мира у свету и заштиту људских живота. Наиме, напади изведени у сајбер простору, преливају се у реални свет, утичући на међународне односе, као и животе људи, а потенцијална штета од сајбер напада може бити краткротрајни прекид свакодневних активности, колапс (у саобраћају, на берзи, итд.), затим, причињавање знатне економске штете, као и катастрофа с великим бројем људских жртава.

Сајбер безбедност је широко коришћен термин, дефинисана на различите начине, често субјективно, а понекад и неинформативно. Сажету дефиницију, која обухвата вишедимензионалност сајбер безбедности и повезује различите дисциплине у решавању сложених изазова сајбер безбедности, дали су *Craigen* и аут. [94]. Према овим ауторима, сајбер безбедност "је обезбеђивање, организовање и прикупљање ресурса, процеса и структура које се користе за заштиту сајбер-простора, као и система који функционишу у сајбер простору, од појава које се *де јуре* не слажу са *де факто* имовинским правима."

Свакако, с обзиром на специфичну природу сајбер напада (контекст примене, тј. мотиве и последице), од изузетног значаја је разматрање безбедности и **одбране рачунарских система** – информационе безбедности у сајбер простору, а која се односи на безбедност информација, тј. на тајност[35], интегритет[36] и расположивост[37] информација [63].

Синтагма сајбер безбедност се често користи наизменично са термином **информациона безбедност**. Иако се умногоме преклапају, ова два концепта нису у потпуности једнака (део 2.2.1). Штавише, сајбер безбедност превазилази границе традиционалне безбедности информација, и обухвата, осим заштите информационих ресурса, и заштиту друге имовине, која укључује и саму особу. У информационој безбедности, људски фактор најчешће се односи на улогу(е) људи у безбедносном процесу. Међутим, у сајбер безбедности људски фактор има додатну димензију – људи могу бити потенцијалне мете сајбер напада, или пак несвесно учествовати у сајбер нападу. Ове чињенице имају етичку импликацију на друштво у целини, јер се заштита одређених рањивих група, за пример деце, може посматрати као друштвена одговорност.

Предузимање злонамерних сајбер активности и повећан сајбер ризик за појединце, организације и владе, утичу на то да сајбер безбедност буде значајни изазов и кључни елемент друштвених, политичких и економских одлука [95, 96]. Обезбеђивање сајбер безбедности је глобално питање [97], а за остваривање циљева

---

[35] Тајност информација подразумева да су информације доступне само овлашћеним лицима.

[36] Заштитом интегритета података омогућава се отклањање могућности промене поруке која се преноси, без обзира на то да ли је ова промена резултат намерног или ненамерног оштећења.

[37] Расположивост се односи на постојање ресурса, тј. сервиса, који обезбеђују овлашћеним корисницима да могу увек, тј. по потреби приступити информацијама/другим ресурсима.

одрживог развоја у хиперповезаном друштву, које се ослања на дигиталну инфраструктуру, веома је значајно повећање свести о сајбер безбедности и снажно партнерство више заинтересованих страна. Стога, током последњих деценија, кључна питања у вези са сајбер безбедношћу су будућа улагања у сајбер-безбедност и начини на који би требало да јавни и приватни сектор третирају ову област [36].

2.2.1. Информациона и сајбер безбедност

Информациона безбедност (*Information security*, INFOSEC) једна је од основних компонената националне безбедности и представља стање заштићености интереса појединца, друштва и државе у информационој области, од различитих ризика/претњи. Овај термин, који је уведен 80.-их година 20. века, представља еволутивну фазу у развоју идеје информационе безбедности, и заменио је раније коришћене појмове – комуникациона безбедност (*communication security*), односно компјутерска безбедност (*computer security*) [79].

Циљ информационе безбедности је обезбеђивање континуитета у пословању и минимизирање пословне штете ограничавањем утицаја безбедносних инцидената [98, 99]. Постоје различите дефиниције информационе безбедности, а концепти и анализе истих, дати су на пример у радовима [26, 100].

Према Међународном стандарду, ISO/IEC 27002 (2005) [101], информациона безбедност је ″очување поверљивости, интегритета и доступности информација. У контексту овог стандарда, информације могу имати различите облике (штампани, писани, електронски, или се преносити поштом/електронски/разговором, итд.).″ [101].

Информациона безбедност, најчешће се дефинише у контексту карактеристика које би требало да поседују безбедне информације, а то су поменуте три особине – поверљивост, интегритет и доступност (*Confidentiality*, *Integrity* и *Availability*, познато као CIA режим троугла) информација [101]. Међутим, ове карактеритике, могу укључивати и додатне, а које би требало заштити, као нпр. тачност, аутентичност, корисност и поседовање [102]. Такође, информациона безбедност није производ/технологија, већ процес [103]. Раније, питање информационе безбедности било је искључиво техничко; данас то није само техничко питање, с обзиром на то да упоредо с развојем рачунара и мрежа, еволуира и процес остваривања њихове безбедности [104]. При свему томе, у циљу заштите информационих средстава и утицаја безбедносног понашања запослених, успостављање информацино-безбедносне културе у овиру компанија/организација и интегрисање безбедносне праксе у корпоративну културу, јесте ″сигуран″ правац деловања [105].

Постоји **разлика** између информационе безбедности и безбедности информационих технологија (или информационо-комуникационих технологија) Према међународном стандарду, ISO/IEC 13335-1 (2004) [106], **безбедност ICT** представља све аспекте који се односе на дефинисање, постизање и одржавање поверљивости, интегритета, доступности, непорицања, одговорности, аутентичности и поузданости информационих ресурса, тј. ICT. Како информациона

безбедност суштински укључује заштиту информационих ресурса, може се закључити да је ICT безбедност подкомпонента информационе безбедности [100].

Разлика у **информационој** и **ICT безбедности** (табела 2) односи се на ресурс/вредност који треба обезбедити; безбедан информациони ресурс може укључивати било који ентитет од кога се информације примају, или коме се информације шаљу, док безбедан ICT јесте сигуран информациони ресурс који је у систему информационе технологије. У системима заснованим на ICT, информације, саме по себи, сматрају се небезбедним, осим ако нису безбедни сви ресурси, као и процеси који се тим информацијама баве.

Табела 2. Информациона безбедност, безбедност информационо-комуникационих технологија (ICT) и сајбер безбедност (преузето и модификовано из [100]

Врста безбедности	Рањивости	Вредност која се напада
Информациона	Различите	информације
ICT	Различите	ICT системи
Сајбер	ICT, информације, итд.	људи и њихови интереси

Дакле, код **ICT безбедности**, вредност, која се **обезбеђује**, јесте технолошка инфраструктура. Код **информационе безбедности обезбеђују** се информације[38], а ICT је инфраструктура која те информације обрађује, чува и преноси (у овом случају ICT, између осталог, представља рањивост, и као таква, мета је различитих претњи у покушају компромитовања информација).

Сајбер безбедност, иако се често користи као синоним за информациону безбедност, разликује се од ње [100]. Као што је поменуто, информациона безбедност је заштита информација од потенцијалне штете, а која проистиче из различитих претњи и рањивости. Сајбер безбедност, с друге стране, није искључиво заштита сајбер простора, већ и заштита свих који функционишу у сајбер простору, као и њихових средстава доступних у/кроз сајбер простор (Табела 1). Тако, сајбер безбедност има веома широк дијапазон значења, од личног до националног. Дакле, **сајбер безбедност** се односи на информациону безбедност у сајбер простору. Овај релативно нови појам, представља еволутивну фазу у развоју идеје информационе безбедности [26]. Различите дефиниције сајбер безбедности су евалуиране у радовима [26, 94].

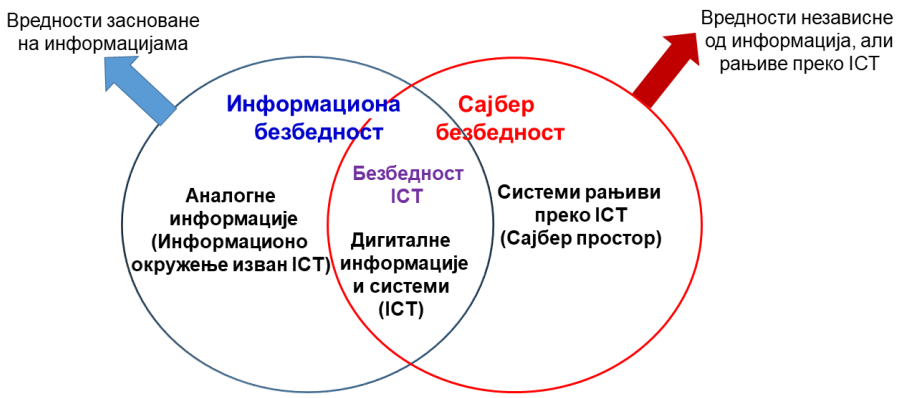
Према ISO/IEC 27032:2012 стандарду, **сајбер безбедност** је ″очување поверљивости, интегритета и доступности у сајбер простору″[107], затим, према Концепту стратегије сајбер безбедности Руске федерације, ″сајбер безбедност представља скуп услова под којима су све компоненте сајбер простора заштићене од максималног броја претњи и утицаја са нежељеним последицама″ [108], или, сајбер безбедност представља ″методе које користе људи, процеси и технологије,

[38] Информација је податак (вредност нечега) са когнитивним значењем, који је могуће интерпретирати у контексту, а који је разумљив за човека/интелигентни систем.

да спрече, открију и поврате од штете поверљивост, интегритет и доступност информација у сајбер простору. Сајбер безбедност настоји да заштити критичну инфраструктуру″ [109].

Чињенице у вези са **сајбер безбедношћу** су да постоје претње, које нису део формално дефинисаног обима информационе безбедности. Специфични аспект сајбер безбедности је заштита интереса особа/друштва/нације (као и њихове имовине, која није заснована на информацијама) од ризика који произилазе из интеракције са сајбер простором [100]. У сајбер безбедности, средства/ресурси које треба **заштити**, тј. вредности које се нападају, укључују све елементе сајбер простора (системе, информације и људе). Тако, у сајбер безбедности, вредности које се обезбеђују су материјална и нематеријална имовина, а која се односи на добробит појединца/друштва у целини. С друге стране, информациона безбедност односи се на безбедност информација, не узимајући у обзир природу и окружење информација (дигитално, аналогно или квантно). Дакле, као што је информациона безбедност шири појам од безбедности ICT [28] и штити информације, без обзира на њихов тренутни облик и/или локацију, **сајбер безбедност** треба посматрати као проширење информационе безбедности. Сајбер безбедност, осим заштите информација/ресурса информационих система и особе/организације, односи се и на заштиту особе(а) која користи ресурсе у сајбер окружењу и заштиту било које друге имовине, укључујући и ону која припада друштву генерално, а која је била изложена ризику као резултат рањивости које произилазе из употребе ICT.

Однос **информационе безбедности** и **сајбер безбедности**, дата је на сл. 2. Елементи првог скупа (левог) су информације (дигиталне, као и аналогне, јер могу бити посредно подложне нарушавању безбедности кроз ICT аналогне уређаје), и њима се бави **информациона безбедност**. Други скуп (десни) обухвата све/свакога чему/коме се може приступити кроз сајбер простор, дакле сваку вредност, која може бити угрожена деловањем кроз или у сајбер простору. Подскуп оба претходна скупа, је скуп ICT система (софтверски и хардверски, тј. информација и техничких система), с рањивостима због којих су подложни угрожавању безбедности ICT система. У случају сајбер безбедности, циљ је да се осигурају сви они који функционишу у сајбер простору, било да су појединци, организације или нације.



Слика 2. Однос информационе безбедности и сајбер безбедности (модификовано и преузето из [100, 110])

Заједничко за све **три врсте безбедности**, информациону, ICT и сајбер безбедност, је то да у свакој од њих постоје фактори **претње**, које их потенцијално угрожавају, као и **рањивости**, а које омогућавају угроженост безбедности. Такође, у свим случајевима се угрожавају својства информација и информационих система. Наведени концепти безбедности разликују се по вредностима/ресурсима, које се штите, и који се примарно угрожавају (окружење у коме се угрожава информациона безбедност): (1) информације у општем контексту, (2) ICT системи, који чувају, стварају и обрађују информације, и (3) информације и системи у контексту и окружењу умреженог сајбер простора [26].

3. САЈБЕР БЕЗБЕДНОСТ ЦИВИЛНЕ АВИЈАЦИЈЕ

> *"Током година, пратећи тренд континуираног пораста обима ваздушног саобраћа, сектор цивилног ваздухопловства прошао је кроз неколико трансформација у сфери дигиталних технологија, у циљу повећања ефикасности и капацитета авио-сектора. С једне стране, то је омогућило одрживост у условима велике брзине пораста авио-саобраћаја, задржавајући неопходну сигурност и безбедност. С друге стране, ови дигитални напретци изложили су авио-сектор претњама по сајбер безбедност, а успешан сајбер напад имао би велике негативне последице на финансије, репутацију, континуитет услуга, па чак и на сигурност и безбедност људи и објеката,"* [23]

Историјски посматрано, **безбедност у ваздухопловству** односи се на заштиту од против-законитих деловања, као што су: против-правна заплена авиона, уништење ваздухоплова у ваздуху током лета, узимање талаца у авиону/на аеродромима, насилни упад у авион/аеродром/аеродромске и друге повезане објекте, уношење оружја или опасних материја у авион/аеродром, коришћење ваздухоплова током обављања редовних операција транспорта путника и робе у циљу угрожавања људских живота, наношења телесних повреда или значајног оштећења имовине/животне средине. Да би се обезбедиле одговарајуће превентивне мере безбедности, неопходно је константно **преиспитивати ниво претњи** и вршити **процене ризика**, узимајући у обзир међународне, националне и регионалне ситуације и окружење. Када претња постоји, потребно је применити унапред одређене превентивне безбедносне мере, и то, сразмерно извршеној процени ризика, као и анализи природе и озбиљности претње. При свему овоме, као нови ризик и изазов за безбедност цивилног ваздухопловства, идентификован је проблем **сајбер безбедности**.

У данашње време ICT, функционисање друштва и привреде, па тако и авио индустрије, у великој мери ослања се на међусобно повезаним рачунарским системима. У сектору **авијације**, ови системи користе се за управљање различитим ваздухопловним операцијама, што поред бројних оперативних бенефита, покреће веома значајна питања у вези са сајбер безбедношћу и налажењем ефикасних одговора на безбедносне изазове својствене огромној мрежи формираној комплексним повезивањем ваздухопловних технологија. Тако, главни **сајбер безбедносни изазови** односе се на технологије управљања ваздушним саобраћајем, *Air Traffic Management* (ATM), рачунарске мреже аеродрома и *e-Enabled* авионе, а сектор авијације, требало би да се проактивно бави свим аспектима (технички, регулаторни и кооперативни) повећања сајбер отпорности целокупног авио система.

Најважније чињенице у вези са **сајбер безбедношћу** у сектору **цивилне авијације** су [4]:

1) сајбер простор интерповезаних и интерзависних система, као и модернизација цивилне авијације, повећава рањивости авиона и авио система, па тако и њихов потенцијални утицај на безбедност

2) сајбер безбедносне рањивости имају потенцијал да угрозе безбедност и ефикасност цивилне авијације
3) константно расту опасности од напада из сајбер простора, што значајно отежава обезбеђивање/одржавање безбедности авио индустрије.

Ризици за цивилно ваздухопловство од злонамерних сајбер активности, повећавају се због тога што сигурносна питања не укључују злонамерне сајбер активности (сигурност *vs.* безбедност), затим, због увођења нових технологија и недостатка искуства, као и међуповезаности и међузависности коришћених система.

Различите **сајбер претње** и врсте сајбер напада карактеришу данашње време, а то је довело до сеизмичких промена у начину на који се приступа тероризму. У контексту авијације, **сајбер тероризам** је ″чудовиште са главом хидре″ [111], који може утицати на ваздушни саобраћај на многобројне начине – сајбер терористички напади могу се користити за ширење дезинформација, за ангажовање у вођењу психолошког рата, као и изазивање страха и невољности за путовањем, што може проузроковати велике економске губитке, а у свом најозбиљнијем облику, сајбер тероризам може довести до губитака људских живота, повреда и великих штета на аеродромима и авионима у току лета.

Као што ће се у будућности, наставити пораст и развој глобалног и националног ослањања људских активности на сајбер простор, тако ће се наставити и континуирани пораст **сајбер претњи**. У овом контекту, дефинисање сајбер безбедносних циљева и постављање оквира управљања, који детерминише улоге и одговорности различитих заинтересованих страна (Влада, законодавац, приватни сектор, грађанско друштво, техничка заједница и академска заједница) у постизању ових циљева је од кључног значаја, нарочито уколико се узме у обзир да ове улоге и одговорности нису прецизно дефинисане међународним законима и стандардима (део 4). Свакако, на националном нивоу, ефикасна и ефективна борба против сајбер претњи је заједничка одговорност у којој јавни, приватни и непрофитни сектори, као и сваки ниво власти, имају веома значајну улогу. Због тога, при идентификацији и реакцији на аномалну активност, сектор цивилне авијације може искористити своје партнерске односе са локалним, државним и савезним агенцијама за спровођење закона, у циљу налажења адекватних одговора и решења.

Најскорије, евидентирани су бројни случајеви нарушавања оперативности авиокомпанија изазвани различитим врстама сајбер напада [112]. Иако су ови сајбер инциденти наизглед малог обима, исти могу имати много веће и озбиљније последице, с обзиром на њихову улогу у авио процесима, као и чињеници да су у сталном порасту. У том контексту, у овом делу дисертације, бавимо се неким од главних питања **сајбер безбедности у цивилној авијацији**, као што су концепт сајбер рањивости сектора цивилне авијације (поглавље 3.1.) и дефинисањем и разумевањем безбедностних сајбер претњи, с нарочитим освртом на познате/доступне примере с којима се већ суочио/суочава авио сектор (систематизовани у делу 7), који илуструју свеприсутност сајбер инцидената и њихов утицај на авијацију, као и релеватност ове дисертације.

3.1. САЈБЕР РАЊИВОСТИ ЦИВИЛНЕ АВИЈАЦИЈЕ

Сектор авијације, осим рањивости на физичке претње, а с обзиром на то да се базира/зависи од веома сложених и интегрисаних технолошких система, поред рањивости на софтверске, хардверске и грешке на рачунарској мрежи, константно је изложен ризику од напада из сајбер простора[39]. Ови сајбер напади могу се остварити преко различитих система, платформи и технологија, које унапређују сигурност и ефикасност путовања. Тако, оперативност и углед целокупног авио сектора, може бити угрожена од стране сајбер преступника[40], који користе сајбер простор, као нову тактику и оружје, с различитим циљевима, као што су саботажа, крађа информација и интелектуалне својине, изазивање нереда и конфузије, итд. При томе, **кључни фактори** који повећавају вероватноћу реализације ових напада, као и потенционално катастрофалне **рањивости** целокупног авио сектора и његових корисника су анонимност нападача, одсуство атрибуције (практично утврђивање одговорности за предузети напад), затим, потребна минимална финансијска средства, као и ограничени одбрамбени механизми. С друге стране, с обзиром на задатак да свакодневно превози милионе путника између различитих географских локација широм света, обезбеђивање и одржавање безбедног функционисања авио система, као једног од најкомплекснијих ICT, јесте приоритет, али и обавеза ваздухопловног сектора.

Чињеница је да ваздухопловни систем, као веома важан ресурс сваке државе, и један од **критичних инфраструктурних система**, потенцијална мета сајбер напада [111]. Ови напади веома су сложени и могу се одигравати на различитим нивоима, у зависности од техничко/технолошких средстава и способности сајбер нападача [34]; напади захтевају адекватну припрему и организацију, затим, употребу софистицираних хакерских алата, као и знања да би се извршили велики поремећаји употребом рачунара, и потенцијално изазову значајна физичка оштећења, као што је нпр. иницирање авионске несреће. Такође, чињеница је и да су сајбер претње на ваздухопловни систем у константном порасту, динамичне су и непредвидиве, а користе их тзв. сајбер терористи[41] у циљу остваривања различитих оштећења авио система – нападима су изложени сви делови авио система, од система контроле летења (*Air Traffic Control,* ATC), преко авиона и авио компанија, до аеродрома и пасошке, као и царинске контроле.

---

[39] Сајбер простор (део 2.1.1.1), представља простор у коме се стварају, складиште, обрађују, размењују и уништавају подаци и информације, коришћењем рачунарских система, који омогућавају умреженост система, процеса и људи на нивоу података [26, 113].

[40] Сајбер напади су глобални проблем, а сајбер преступници користе сајбер простор за предузимање различитих незаконитих активности и остваривање својих циљева (тероризам, криминал и злочин против појединца/компаније) [91].

[41] Сајбер терориста је особа, која има непријатељске намере, знање из области IT и приступ поверљивим IT информацијама. Актери сајбер тероризма могу бити терористичке организације (*Al-Qaeda, ISIS, Irish Republican Army, Liberation Tigers of Tamil Eelam, Shi'ite Islamic group, Kataib Hezbollah,* итд.), симпатизери терористичких организација (особе који подржавају идеологију теророристичких организација, али нису активно укључени у *online* терористичке активности), као и "тражиоци сензације", *thrill seekers* (особе, тј. хакери чији мотиви за напад нису политичке/идеолошке природе, већ им је примарни мотив стицање славе, тј. тежња да прославе своје име (псеудоним) извођењем сајбер напада, који захтева врхунске IT вештине [114].

На пример, енормни пораст[42] broja **IoT**[43], који се користе у транспортном саобраћају, узрокује и повећање простора за предузимање сајбер напада на IoT системе, а који најчешће не располажу адекватном анти-спам/анти-вирусном заштитом [116]. Такође, рањивост на сајбер претње у вези су и са порастом употребе, уређаја као што су *iPhones, iPads* и *Anroid,* тј. *Bring Your Own Device* (**BYOD**)[44], који се могу потенцијално користити за прикупљање поверљивих компанијских информација, или могу бити извор рачунарских вируса, с обзиром на то да ови уређаји имају комуникацију с екстерним системима. У сваком случају, одговорност за безбедност информационих система подједнако деле државни и приватни сектор, као и појединци, а за одржавање безбедности и сигурности ових веома разгранатих рачунарских мрежа, неопходна је координисана активност бројних служби, агенција, као и приватних компанија. Дакле, да би се изградио јединствени **безбедносни оквир** за сајбер безбедност, неопходна је заједничка стратегија, која би требало да укључи све безбедносне слојеве, тј. обуку и свесност, превенцију, истраживања и детекцију, реаговање и опоравак [117], као и остваривање сарадње између стручњака из области сајбер безбедности [118].

И пред увођења многобројних мера, као и значајних инвестирања у побољшања безбедности операција цивилног ваздухопловства на глобалном нивоу, **безбедност авио сектора** и даље је критична област и фокус свих заинтересованих страна. Иако су након терористичких напада 11. септембра 2001. године (познатог као **напад 9/11**) у USA, уведени бројни нови безбедносни стандарди и препоручене праксе и нове безбедносне мере[45] (*Standards and Recommended Practices* (SARPs) у складу са *International Civil Aviation Organization* (ICAO) [120], након тога, догодили су се бројни **авио-инциденти**, као нпр. претња течним експлозивом (2006) и бомбом (2009). Наиме, према саопштењима британских власти (август, 2006) **осујећена је терористичка акција**, и ухапшени актери, чији је циљ био физичко уништење авиона на десетини летова из UK у USA, као и Канаду, коришћењем течног

---

[42] Број IoT уређаја непрекидно расте: 2021. год. било више од 10 милијарди IoT, а очекује се да ће до 2025. године, глобално генерисање података бити веће од 73 зетабајта (73 трилиона гигабајта) [115].

[43] IoT [47], као што је детаљно објашњено у делу 2.1.1.2, представља скуп ствари/физичких објека (технологије, уређаји и алати), који захваљујући постојећој електроници, сензорима, софтверу и конекцији, омогућавају размену података с произвођачем, оператером и/или другим повезаним уређајима, са било ког места (географске локације), у било које време. Ова размена података, између људи, ствари, као и људи и ствари, остварује се интернет везом и интернет протоколом адекватног капацитета (део 2.1.1.2).

[44] *Bring Your Own Device* (BYOD) јесте назив за уређаје, као што су *iPhones, iPads, Anroids* и *Tablets.* Користе се и називи: *Bring Your Own Technology* (BYOT), *Bring Your Own Phone* (BYOP), као и *Bring Your Own Personal Computer* (BYOPC), и односе се на политику одређених компанија, која подразумева дозволу употребе поменутих уређаја (у власништву запослених) на радном месту, а тако и коришћење привилегованих компанијских информација и апликација (тзв. IT ″конзумација″).

[45] Последице терористичког напада 9/11, биле су крупне друштвене промене у USA (2001–2008. године), које су подразумевале пооштравање мера за очување националне безбедности и формирање (2002) Министарства унутрашње безбедности, *Department of Homeland Security* (DHS) са значајним надлежностима [119], што је и довело до увођења нових стандарда, који су се односили на поштовање/непоштовање права на приватност грађана USA.

експлозива на бази водоник пероксида. Ову безбедносну претњу глобалној цивилној авијацији, открила је британска полиција током опсежне операције надзора. Аеродроми су након тога, променили правила о томе шта путници могу да унесу у авион у ручном пртљагу (у већини држава, боце с течношћу, гелом или кремом, веће од 100 mL су забрањени за ручни пртљаг) [121]. Други поменути инцидент био је **покушај напада** на **авион** *Airbus* A330 на лету 253, компаније *Northwest Airlines* са 279 путника, 8 стјуардеса и 3 пилота, непосредно пре слетања на аеродром *Detroit Metropolitan* након трансатлантског лета из Амстердама (25. децембар, 2009). Приписује се терористичкој организацији *al-Qaeda* (AQAP), а предузео га је 23-годишњи држављанин Нигерије *Umar Farouk Abdulmutallab*, користећи хемијски експлозив (пластични експлозивни прах и киселина као катализатора реакције) [122]. На овом лету није било ваздухопловних маршалера, а неколико путника и чланова посаде осујетило је ову терористичку акцију, која је могла имати фаталан исход. *Abdulmutallab* је због своје улоге у завери, осуђен на доживотну затворску казну, без могућности добијања условне слободе [123].

Такође, и **покушај уништења авиона** коришћењем импровизоване експлозивне направе сакривене у кертрицима за штампаче [46] још је један пример инцидента, у коме је коришћен експлозивни уређај (*Improvised Explosive Device,* IED). Затим, инцидент у коме је коришћен IED сакривен у лаптопу[47], указују на то да терористи, за постизање својих циљева, настављају да трагају за новим начинима извођења напада на операције цивилног ваздухопловства.

Суочен с бројним новим безбедносним претњама, па тако и претњама од сајбер напада, сектор **цивилне авијације** би требало да се практивно бави решавањем креираних безбедносних питања, као и оних у вези са сајбер безбедношћу. Као што је детаљно анализирано у поглављу 2.2, **сајбер безбедност** представља ″очување поверљивости, интегритета и доступности информација у сајбер простору″ [128]. **Циљ сајбер безбедности** јесте да се корисник и/или власник информација и информационих система, одбрани од сваке врсте сајбер напада, без обзира на то да ли је позната или није атрибуција нападача, да ли су напади откривени или нису,

---

[46] За извођење терористичких напада, оперативци *al-Qaeda* (AQAP) користе различите врсте импровизованих експлозива и експлозивних уређаја (*Improvised Explosive Device*, IED). Тако је конструисан IED, који се веома тешко детектује, користећи кертрице за штампаче у коме је било сакривено 400 g пентаеритритол-тетранитрата (PETN), експлозивне супстанце (нитратни естар пентаеритритола), структурно веома сличне нитроглицерину. IED су били намењени да експлодирају на летовима теретних авиона из UK за USA (октобар 2010. године). Куриозитет је, да су IED пронађени као резултат обавештајне операције, а не као резултат безбедносне провере, што је изазвало значајну забринутост у вези са способностима терориста да избегну постојеће софистициране безбедносне противмере. [124–127].

[47] Радници међународног аеродрома у Могадишу, а које је регрутовала терористичка организација *al-Shabaab*, успели су да прокриумчаре лаптоп са експлозивном направом (фебруар 2016), која није откривена на пункту за контра-диверзиону (KD) контролу. Терористи су, затим, на терминалу за укрцавање предали саучеснику лаптоп, и преусмерили га на *Daallo Airlines Flight* 159 за Џибуту (лет авиона *Turkish airlines*, отказан је у последњем тренутку). Двадесет минута након лета, лаптоп је експлодирао, али су пилоти успели да се врате на аеродром и принудно слете [127].

као и независно од тога ко је одговоран за напад (држава, недржавна организација, група/појединац).

Анализа постојећих и евалуација сајбер претњи у авио сектору, указују на неопходност координације и међународних споразума о налажењу глобалних решења у вези са сајбер безбедношћу у ваздухопловству [4], с обзиром на то да је овај систем потенцијална мета за извођење сајбер напада великих размера у циљу крађе информација, остваривања профита, хактивизама,[48] итд.

3.1.1. Цивилна авијација и информационо-комуникационе технологије

Интензиван и континуирани развој информационих и комуникационих технологија/система, одражава се и на развој ваздухопловне индустрији. Пораст броја путника, развој нових, већих и модернијих аеродрома (**"паметни" аеродроми**[49]), као и увођење нових и софистицираних авиона, свакако ће резултирати и већом употребом ICT, као и напреднијих компјутерски заснованих система у свим аспектима операција цивилног ваздухопловства. Ово је нарочито појачано тежњом да се смање трошкови, повећа ефикасност, као и оствари синергија између свих заинтересованих страна (државни и приватни сектор, као и појединци). Дакле, у сталном стремљењу ваздухопловне индустрије да унапреди и побољша перформансе својих процеса/операција на најекономичнији начин, ICT има значајну улогу, јер се само стратешком, интензивном и иновативном употребом ICT у будућим политикама и програмима развоја, могу остварити постављени циљеви, као што је нпр. појадностављивање процеса путовања, повећање удобности и безбедности путовања, итд. Тако, многи аеродроми и авио компаније уводе ефикасније начине за пријављивање путника, као што је коришћење мобилних уређаја (нпр. *Personal Digital Assistants*) за електронско издавање карата, *check-in* и имиграционо одобрење.

Развој ICT повезан је са свим сегментима система цивилног ваздухопловства, од побољшања система за **праћење, навигацију** и **комуникацију**, преко апликација које користе пилоти за примање, складиштење и приказивање релевантних информација неопходних за доношење одлука у кокпиту, до информационо-технолошких решења за продају авио карата и забаву путника у авиону. Тако, развијене **нове технологије**, у циљу подршке постојећим системима авиона, су нпр. бежичне компоненте за летење (*fly-by wireless* компоненте), забаву путника (*In Flight Entertainment*, IFE), као и управљање ваздушним саобраћајем базираном на *Global Positioning System* (GPS) извештајима и комуникацији између пилота и контролора летења преко *data link* сателитских система [131]. У целој архитектури система цивилног ваздухопловства, постоји огромна зависност од

[48] Хактивизам (видети Табелу 1) је хаковање *web* странице/рачунарске мреже у циљу преношења друштвене или политичке поруке (хаковање с циљем) [129].

[49] Паметни аеродроми су аеродроми који у великој мери користе аутоматизацију и дигиталне технологије, као што су услуге за путнике с мобилном подршком, паметни гејтови, имплементација аеродромских оперативних командних центара (*Airport Operations Command Centers*), извештавање о свим аспектима рада аеродрома, итд. Ови аеродроми пружају различите услуге и сервисе, као што су системски генерисана упозорења и обавештења, могућности *self*-сервиса на захтев (како за путнике, тако и за особље), циљане промоције и понуде специфичне за кориснички профил, итд. [130].

рачунарских и IT система, с израженим трендом пораста ове зависности у времену које долази.

У сектору авијације, након 1960. године, уведени су бројни нови системи, као и успостављене нове стандардне процедуре, дајући пилотима и контролорима лета прецизније навигационе информације. Тако, **савремени системи и концепти**, као што су *Instrument Landing System* (ILS), *Microwave Landing System* (MLS), *Area Navigation* (RNAV) и *Global Navigation Satellite System* (GNSS), омогућавају ефикасније праћење путање лета, уз уштеду времена и горива, и обезбеђују тачност летачких процедура.

С друге стране, повећања нивоа интеграције алата ICT у механичке уређаје, који се рутински користе у ваздухопловној индустрији, уводи нове сајбер безбедносне ризике, као што је креирање концепта аутономног летења за ***e-Enabled* авионе** (*Boeing* B787, *Airbus* A380 и *Airbus* A350). *E-Enabled* (″повезан″) авион, генерално означава побољшане оперативне могућности авиона, инкорпорирањем напредних ICT у авио систем. Ови авиони са напредним сензорским, рачунарским и комуникационим карактеристикама, имају високо интегрисане интерконектоване софтвере и рачунарске системе контролисане фирмвером[50] са специфичним рачунарским и контролним задацима у реалном времену; TCP[51]/IP везе омогућавају пренос података у ваздуху (током лета) и на земљи, као и добијање информација у вези с критичним операцијама (контрола, навигација, оперативност и одржавање). TCP/IP *data links* у лету, као и на земљи, преносе и примају критичне информације о контроли, навигацији, операцијама и одржавању. Дакле, u овом новом концепту, тј. *e-Enabled* авиону, предвиђено је да све кључне ваздухопловне апликације и услуге буду повезане у јединствен интегрисани комуникациони систем изграђен коришћењем бројних технологија, као нпр. IP, GPS и других радио-фреквентних (RF) система [132]. Први комерцијални *e-Enabled* авион на свету конструисала је компанија *Boeing* (авион типа 787 *Dreamliner*), који комбинује снагу интегрисаних ICT система за повећање оперативне ефикасности и финансијских прихода, као и поједностављење одржавања авиона [133]. С обзиром на то да су *e-Enabled* авиони компјутеризовани и имају јединствене захтеве за умрежавањем, безбедношћу, сертификацијом, као и физичке оперативне захтеве, интеграција ових авиона представља ″застрашујући″ изазов [132]. *E-enabled* авион има могућност репрограмирања компоненти авионске опреме (критичне за лет) бежичним путем, или коришћењем различитих механизама за пренос података. Због тога, као и због могућности повезивања путника на мрежу *e-Enabled* авиона, овај авион је изложен сајбер безбедносним рањивостима, услед намерне/ненамерне корумпираности података и/или система који су критични за безбедност и континуирану пловидбеност авиона. Дакле, концепт аутономног летења за *e-Enabled* авионе доводи до пораста сајбер рањивости авиона. Тако, након несреће етијопијског авиона *Boeing* 737 MAX 8 (2019), у којој је 157 особа изгубило живот, сви *Boing-*

[50] Фирмвер (*firmware*) представља посебну врсту софтвера, тј. софтвер посебно дизајниран за комад хардвера, као што је нпр. паметни телефон, матичну плочу рачунара, даљински управљач, итд.

[51] TCP (*Internet Transmission Control Protocol*), обезбеђује контролисан проток, тј. поуздан, двосмерни пренос података.

ови авиони овог типа су приземљени (више од 300) [133]. Опис и анализа ове авионске несреће дата је у делу 7.

Такође, употреба различитих софтвера (npr. *Commercial-Off-The-Shelf* софтвер (**COTS**)[52], као и интеграција авиона и *off-board* система (АТС станице, сателитске комуникације, итд.), представљају безбедносне изазове и условљавају креирање оквира за очување безбедности сајбер-физичких система[53] [134]. Поред тога, унапређење комуникације коришћењем ваздухопловних мрежа, као и међузависност укључених система повећава број сајбер рањивости и безбедносних питања, као нпр. код система који се користи за надзор ваздушног саобраћаја (*Automatic Dependent Surveillance Broadcast*, ADS–B). Показано је да **ADS–B систем** има дизајнерске пропусте са недовољно јасним потенцијалним утицајем на авион. Наиме, ADS–B представља главну потенцијалну ″површину напада″, која је отворена за различите врсте сајбер напада. Овај систем (детаљно описан и анализиран у делу 6), користи се за аутоматски пренос и пријем података у вези с положајем и идентификацијом авиона (користи се и за добијање додатних информација за популарне онлајн сервисе за праћење летова као што је Flightradar24). ADS–B има кључну улогу у поједностављивању АТС операција, при чему је безбедност авио-операција од изизетног значаја. Међутим, велики део података који се преносе коришћењем ADS–B обављају се у нешифрованом формату и стога су посебно осетљиви на прислушкивање, пресретање и, потенцијално, на ометање и измене од стране трећих лица. За борбу против ове претње стручњаци су предложили против-мере, које укључују шифровање ADS–B података и насумично ″замућивање″ података о авиону, тако да искључиво АТС и оператери авиона добијају одређене информације/податке, док их други, тј. трећа лица, не могу добити.

Свакако, сајбер рањивости у цивилном ваздухопловству, у вези су са сложеношћу авио система, која укључује више линија програмског кода (*lines of code*, LOC[54]), као и величином софтвера који га подржава, што све смањује могућност тестирања софтвера, тако повећавајући рањивости система. Такође, софтвер током ″живота″ авиона, пролази кроз бројне процесе ажурирања и ремонта, што може, и поред нарочите пажње, узроковати безбедносне ″багове″ у софтверу. Поред тога, најновији авионски софтвери користе предности COTS компоненти, а што потенцијално може довести до тога да хакер продре у ″срце″ авио система.

---

[52] COTS – софтверски и хардверски производи, направљени и доступни за широку употребу/продају; дизајнирани су тако да се једноставно имплементирају у постојеће системе, без потребе за прилагођавањем. На пример, *Microsoft Office* је COTS производ, тј. ″упаковано″ софтверско решење за компаније.

[53] Сајбер-физички системи су инжењерски системи који су изграђени и зависе од синергије рачунарских и физичких компоненти. Тако, у савременим ваздухопловним система, постоји чврста веза између сајбер система (нпр. обрада података, комуникација, итд.) и физичких елементата (нпр. сензори, окружење, итд.).

[54] LOC је метрика софтвера и квантификује величину рачунарског програма, изражену бројем линија у тексту програмског кода.

Дакле, у авио систему и *e-Enabled* авионима, мрежа *onboard* сензора и актуатора[55] има жичане и бежичне чворове, који врше мониторинг и контролу унутрашњег и спољашњег окружења авиона, као и *on-board* физичких компонената и средстава. Стога је неопходно вршити константне процене рањивости жичаних и бежичних чворова и мреже (системи кабинских услуга, уређаји за посаду, информативне услуге авио-компаније, информације о путницима, услуге забаве и системи одржавања, итд.) затим, бежичног линка за пренос података, као и ATC, сателитских комуникација и *Airline Info Services Domains* [135].

Свакако, бројни су **бенефити интеграције ICT** мреже авиона са системима на земљи (нпр. летачке и кабинске операције) и ICT инфраструктуре, а односе се на оперативну ефикасност, удобност путовања, одржавање и ремонт. Тако, системи ових авиона шаљу своје податке, користећи сателитске везе или земаљске комуникационе мреже, до сервиса за обраду података, који снабдевају авио-оператере подацима у реалном времену, а што доприноси побољшању бројних авио-услуга. С друге стране, поред бенефита од ових IoT података о актуелној ситуацији, постоје значајни **безбедносни изазови** при конекцији ових система на комуникациону мрежу, а односе се на потенцијалну могућност путника да намерно или случајно интегрише небезбедне податке/системе, као и с тим у вези, правни аспекти ових активности и правна питања, као што је повреда приватности података [136]. О свему овоме је неопходно размишљати током читавог ″животног циклуса″ комуникационе мреже. Такође, при свакој интерној или екстерној интеракцији, које се остварују преко комуникационе мреже, неопходно је вршити процене ризика, тестирање претњи, као и предузимати одговарајуће активности за њихово ублажавање.

Опасности за **авио системе**, осим што су реалне, у сталном су порасту. Тако, аеродромске рачунарске мреже рањиве су на сајбер нападе преко различитих **сајбер система** и **физичких елемената**, као што су USB драјвови и уређаји, лаптопови, бежичне приступне тачке, уређаја запослених, ″паметних″ телефона, е-поште, социјалних мрежа, инлајн превара, дистрибуираних DDoS напада, итд. [137]. *Denial of Service* (DoS) (део 2.1.2), је врста сајбер напада у коме злонамерни сајбер преступник, покушава да онемогући, другим корисницима, приступ сајту, сукцесивно шаљући захтеве (с погрешном адресом) за аутентификацију, а што доводи до потенцијалног преоптерећења сервера. Сложенији напади су тзв. дистрибуирани DoS напади, тј. DDoS, који се остварују истовремено с више извора. У DDoS нападу, малициозни сајбер преступник врши напад на сајт – мету, тако што креира „војску” тзв. зомбија или робота (рачунара), који су под контролом нападача у циљу онемогућавања рада сервера. Да се овај циљ не би остварио, администратори привремено искључују нападнути сајт који тако постаје недоступан. Тиме је циљ нападача остварен, али су сервер и остали сајтови које хостује и даље у функцији.

[55] Актуатор (покретач) је уређај који покреће или управља неким механизмом. Покретач претвара управљачки сигнал у механичко деловање, као што је електрични мотор. Покретачи се могу заснивати на хидрауличким, пнеуматским, електричним, термичким или механичким средствима, али их све чешће покреће софтвер.

Бројни су **хакерски напади** на све делове авио сектора, као што су нпр. сајбер инциденти на аеродромима, који су у вези са *Private network baggage* системом. Овај систем изложен је различитим врстама сајбер напада, као нпр. напади *zombie army*[56], *malware*[57]-а или *botnet*-а[58] (део 2.1.2), а који проузрокују да безбедна приватна мрежа постаје јавна[59] [137]. **Сајбер претње**, као што су поменути рачунарски вируси и малициознији напади на рачунарске системе сектора авијације, у сталном су порасту, као што доказују и извештаји *McAfee Labs*[60], водеће светске лабораторије за истраживање сајбер претњи. [139], као и извештаји *European Organization for the Safety of Air Navigation* (EUROCONTROL)[61]-а [141].

---

[56] *Zombie army* је назив за скуп рачунара који су повезани интернетом; програмирани су тако да шаљу *spam* без знања и одобрења власника рачунара.

[57] *Malware* – рачунарски програми који су дизајнирани тако да се инфилтрирају и оштећују рачунар – мету без знања и одобрења корисника рачунара (део 2.1.2). То је и општи термин, који обухвата различите врсте рачунарских претњи, као што су *trojan horses* (хакер може приступити другом рачунарском систему–мети преко интернета у циљу прикупљања/крађе поверљивих информација, инсталирања софтвера, креирања и модификације фајлова, DDoS напада, итд.), *computer spyware* (сам себе копира на више система и, користећи мрежу, сам себе дистрибуира свим умреженим рачунарима; то су тзв. компјутерски црви, који се шаљу нпр. преко USB флеш меморија, *peer-to-peer* апликација, али и преко сајтова за друштвено умрежавање, као што је *Facebook*), *rootkits* (омогућава хакерима да анонимно приступе различитим оперативним системима, као што су *Microsoft Windows, Linux, Mac* и *Solaris*; често мењају делове оперативног система или инсталирају себе као драјвере) и *spyware* (врста *malware,* који скупља податке о корисницима, без њиховог одобрења; *spyware* се углавном инсталира на рачунар, без знања корисника система, али се може инсталирати од стране администратора на неком дељеном рачунару, у циљу тајног мониторинга осталих корисника.

[58] *Botnet* (део 2.1.2), има најчешће негативну/злонамерну конотацију, а његова величина пропорционална је штетном ефекту напада – уколико је већи, већи је и штетни ефекат напада, као и драстичније онеспособљавање сајта. Данас је на интернету могуће и изнамљивати *botnet*-ове (тзв. DDoS-*as-a-service)*. Постоји могућност креирања *botnet-а* и без знања корисника рачунара, нпр. дистрибуцијом, тј. *Download-ом malware* и *spyware*. При томе, уколико се *download*-ује неки малициозни код/програм, рачунар корисника може постати робот, који може инструкцијама свог "господара из сенке" бити активиран у циљу предузимања злонамерних напада на неки циљани сајт.

[59] Виртуелна приватна мрежа (*Virtual Private Network,* VPN) је технологија, која омогућава сигурно повезивање приватних мрежа у заједничку виртуелну приватну мрежу преко јавне мрежне инфраструктуре. Код VPN, за разлику од традиционалне мреже, подаци који се преносе су заштићени криптографски, тако да VPN мрежа обезбеђује поверљивост и интегритет података. VPN потенцијално може бити угрожена различитим врстама сајбер напада (напади аутентиофикације, криптографски напади, фалсификовање сервера, итд.). Ова мрежа има велику примену у корпоративном окружењу, као и државама које прописују строжије регулативе за интернет садржаје, тако да је VPN популаран начин заобилажења ограничења.

[60] *McAfee Labs* критички анализира концепте сајбер претњи у реалном времену и врши експертизу у вези са максимизирањем заштите и минимизирањем безбедносних сајбер ризика [138].

[61] EUROCONTROL (основана 1960) је паневропска (сачињава је 41 европска држава), цивилно-војна организација, која у сарадњи с националним органима цивилног ваздухопловства сваке државе чланице, агенцијама и провајдерима ATM/ATC, затим, корисницима цивилног и војног ваздушног простора, као и индустријским сектором и одређеним европским институцијама, углавном је ангажована на развоју и одржавању ефикасног европског система управљања ваздушним саобраћајем [140].

Тако, на пример, током 2020. године, било је 62 сајбер-напада *ransomware*-а на сектор авијације, а 2021. су постављени нови рекорди са захтевима од 50 милиона долара [142]. ***Ransomware*** је врста *malware*-а, тј. злонамерни софтвер, који енкриптује фајлове мете и затим захтева новац (откуп) за њихово безбедно враћање, тј. приступ фајловима. Генерално, постоје два типа *ransomware*-а, и то су **криптори** (енкриптују фајлове и тако их чине недоступним; за декрипцију фајлова потребан је кључ коришћен при енкрипцији, и за то се плаћа откуп) и **блокери** (блокирају рачунар или други уређај, тако га онеспособљавајући). *Ransomware* је често дизајниран да се шири на мрежи и циља базу података и сервере датотека, тако да може, веома брзо, онеспособити целу компанију/организацију. То је растућа претња, која наноси значајну штету и трошкове компанијама/организацијама.

Због пораста глобалног сектора авијације, повећањем броја путника у авио саобраћају, развојем већих и нових, тзв. **паметних аеродрома** (фуснота 49), као и увођењем софистициранијих авиона, императив авио индустрије је дефинисање и имплементација сразмерних стратегија сајбер заштите од злонамерних претњи, које угрожавају оперативни интегритет ове кључне индустрије. Дакле, авио индустрија ће морати да развија нове приступе у остваривању сајбер безбедности, јер – већи број корисника, значи више података, већи број уређаја, као и ″облака″, што проузрокује настанак ″савршене олује сајбер претњи и рањивости″[62] [143].

При свему овоме, од великог значаја је развијање **концепта сајбер безбедности** у ваздухопловству, дефинисаног од стране ICAO (документ 9985) [144], који се односи на безбедност информационих и комуникационих система, технологија и њихове примене [1]. То укључује аналогне и дигиталне уређаје, радио станице, телекомуникације, рачунаре, рачунарску опрему и софтвер, систем за складиштење података и уређаја, сателитске системе, системе надзора, навигационе системе, као и различите, с њима повезане, услуге. ICAO, као једна од лидера, одговорна за постављање регулатива и смерница у вези са сајбер безбедношћу (део 4), улаже велике напоре у циљу обезбеђивања адекватног *set-up*-а да би *Aeronautical Telecommunication Network* (ATN) заснован на *Internet Protocol Suite* (IPS), за остваривање поуздане комуникације (авион–авион и авион–земља). Веома је важно истаћи да мреже и чворови у авијацији немају сличности са стационарним рачунарским мрежама на земљи. ATN је *ad-hoc* бежична мрежа, која има бројне мобилне чворове, а ова мобилност представља ″најслабију карику у ланцу″, и може се искористити у циљу угрожавања апликација, које се користе за комуникацију.

Да ли се могу спречити намерни малициозни хакерски напади на сектор авијације? Иако су ризици константни, а хакери изузетно прилагодљиви, отпорност на нападе, може се повећати ефективном способношћу искусног пилота да донесе праву одлуку, када уочи необичну ситуацију. Поред тога, веома је значајно разумевање платформе за хакерске нападе, а то значи да би требало поставити јединствени репозиторијум претњи на софтвер/хардвер, уочене од стране програмера и стручњака за сајбер безбедност. Ове структуиране податке требало

[62] На пример, у 2020.-ој, у односу на претходну годину, било је 530 % више пријављених сајбер инцидената у ваздухопловној индустрији [142].

би ажурирати (регулаторне агенције као што су ICAO и FAA), и тако их учинити доступним у различитим развојним платформама.

Како упозоравају бројни стручњаци за сајбер безбедност, напади злонамерних хакера на авио систем, могу имати катастрофалне последице. Након авионске несреће (2008) на *Spanair flight* 5022, установљено је да је централни компјутерски систем, који се користи за мониторинг техничких карактеристика авиона, био заражен *malware*-ом. Затим, комуникациони системи ваздухоплова са слабом енкрипцијом, изазвали су дебате у вези са безбедношћу и приватношћу порука, које се размењују преко *data-link* система. Такође, систем који емитује позицију ваздухоплова, може бити потенцијално компромитован од стране висококвалификованих хакера. Поред тога, на основу признања једног од званичника DHS-а да су он и његов тим даљински "упали" у *Boeing* 757 (2017), закључено је да се хаковање авиона може извести једноставније, него што се до тада претпостављало [145].

3.1.2. Кључне сајбер претње у цивилној авијацији

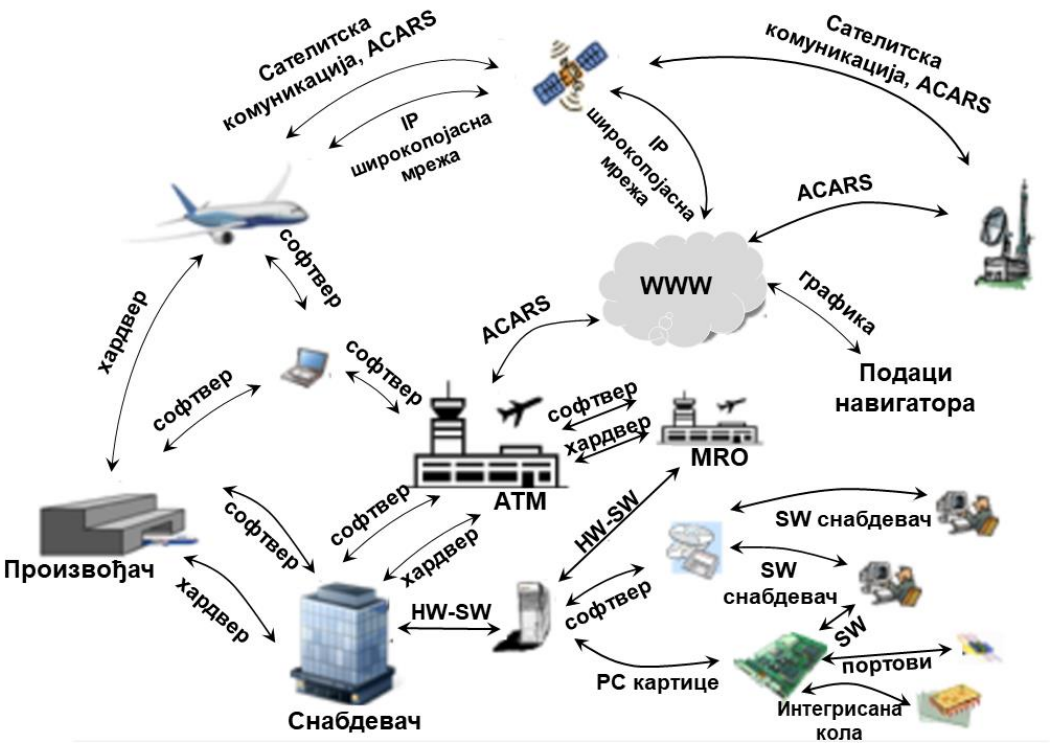
Авијација, као једна од критичних националних инфраструктура, захтева веома висок ниво свих слојева безбедности, од обуке и свесности ситуације, преко, превенције и истраживања, до откривања, реаговања и опоравка. Иако ваздухопловна индустрија иде у корак са напредним ICT и веома брзо их усваја, и то углавном безбедно, свако ново побољшање корисничких сервиса или повећање ефикасности авио операција, отвара простор сајбер криминалцима да искористе ту нову/унапређену технологију, за личну, а понекад и политичку добит. Учесталост сајбер напада расте, као и ниво софистицираности нападача, а без кохезивног и јединственог приступа проблему, изгледа неизбежно да потенцијални сајбер напад с разорним и евентуално фаталним исходом, буде и успешан, нарочито уколико се не заустави релативно брзо.

Савремени авио-системи користе процесорске хардвере и заједничке хардверске платформе за хостинг функционалности софтвера. Специфични интерфејси авиона, једноставно се конектују са COTS (фуснота 52) технологијама, тако да ICT обухвата цео авио систем, од пројектовања авиона, преко летачких операција, одржавања, комуникације и навигације, до контроле летења.

На слици 3, приказано је информационо и комуникационо-технолошко (ICT) окружење авио система.

Ваздухопловни систем се састоји од подсистема и бежичних технологија, који омогућавају три главне апликације, а то су комуникација, навигација и надзор [147]. Пилоти користе комуникационе протоколе (као што су веома високе фреквенције (VHF), високе фреквенције (HF) и *Controlled Pilot Data-Link Communication* (CPDLC) за размену информација (вербалних или заснованих на порукама) са земаљском станицом и сателитом. Затим, користи навигационе протоколе, као што су VHF *Omni-directional Range* (VOR), *Instrument Landing System* (ILS) и *Distance Measuring Equipment* (DME), за летачке операције. Земаљска станица користи протоколе за надзор, као што су *Primary Surveillance Radar* (PSR), *Secondary*

Surveillance Radar (SSR) и *Automatic Dependent Surveillance-Broadcast* (ADS-B) (део 6), који су увек активни током прелета и слетања авиона.



Слика 3. ICT окружење авио система (преузето и модификовано из [146])
HW – хардвер; SW – софтвер

Air Traffic Management (ATM) представља динамично, интегрисано управљање ваздушним саобраћајем и ваздушним простором, укључујући услуге ваздушног саобраћаја, управљање ваздушним простором и управљање протоком ваздушног саобраћаја – безбедно, економично и ефикасно, кроз обезбеђивање објеката и услуга у сарадњи са свим заинтересованим странама, и укључујући функције у ваздуху, као и на земљи [148].

ATM се састоји из три главна сервиса:

- *Air traffic services* (ATS) – за остваривање безбедног и неометаног тока саобраћаја (уз помоћ ATC), обезбеђивање потребних информација летачким посадама (*Flight Information Service*, FIS) као и, у случају ванредне ситуације, одговарајућим органима/службама; ATS се ослања на тактичке интервенције контролора летења и директну комуникацију с летачким посадама, најчешће, током целог лета.
- *Air Traffic Flow Management* (ATFM) – за ефикасније регулисање промета ваздушног саобраћаја, како би се избегла загушења појединих контролних сектора; ATFM мере су пре-тактичке, јер не утичу на тренутну ситуацију, већ на блиску будућност.

- *Airspace Management* (ASM) – за ефикасније управљање ваздушним простором, како би се задовољили бројни корисници овог простора (цивилни и војни); ова услуга односи се на начин додељивања ваздушног простора различитим корисницима (путем рута, зона, нивоа лета, итд.), као и на начин његовог структуирања у циљу пружања услуга ваздушног саобраћаја.

АТС се повезује с земаљским мрежама и *data* центрима, при чему су *data* центри повезани с интернетом. Земаљске мреже омогућавају сателитске, као и авионске мреже. Функционисање авио-система доминантно се заснива на повезивању земаљске станице и авиона. Земаљска станица се састоји од АТС који је у вези с пратећим земаљским јединицама (*data* центри, земаљски радари и торњеви).

VHF и CPDLC омогућавају комуникацију и између авиона и АТС [149]. VHF обезбеђује гласовну комуникацију, док CPDLC, користећи VHF *datalink*, обезбеђује комуникацију засновану на порукама. *Digital Satellite Communication Networks* (DSCN) омогућавају повезивање са сателитима, и користе се за комуникацију, као и навигацију. DME, VOR и ILS, користе се за навигацију и *smooth* слетање. DME одређује растојање између авиона и радио-навигационог средства. VOR функционише на кратким растојањима и омогућава одређивање позиције авиона, као и одржавање жељене трајекторије. ILS омогућава навођење током фазе инструменталног прилаза и слетања. PSR и SSR се користе за надзор и детектовање ваздухоплова. Такође, увођење ADS-B система је најновији допринос ефикасном надзору ваздухоплова међусобно, као и ваздухоплова и земаљских станица. Ове основне протоколе, користе ваздухопловни системи за несметане операције ваздушног саобраћаја.

Главне потенцијалне **мете**, које би могле бити у фокусу сајбер напада на **цивилно ваздухопловство** су [146]:

- интерни аеродромски компјутерски системи
- *in-flight* системи за управљање авионом
- АТМ системи [150]

Системи **аеродромских објеката**, као што су организациони системи и ентитети, који рутински користе интернет за обављање свакодневних операција (размена података, слање порука, итд.), нарочито су рањиви на сајбер претње. Осим ових, сајбер рањивостима изложени су и системи за надзор и прикупљање података (*Supervisory Control and Data Acquisition*, **SCADA**)[63] [152], који су у срцу дистрибутивне критичне инфраструктуре аеродрома, и често се користе за контролу транспорта пртљага, вентилационих система, итд. Пораст употребе мобилних апликација повезаних с интернетом, доводи и до пораста потенцијалних рањивости на нападе бројних физичких уређаја (USB, рачунари, дигиталне камере, итд.) и сајбер оперативних активности (DoS, *phishing*, *trojans*, itd.). [137].

[63] SCADA системи су агрегација програма и техничких средстава, који омогућавају контролу (локалну или даљинску) параметара аутоматизованих технолошких процеса; SCADA омогућава комплексно праћење, прикупљање података у реалном времену и њихово евидентирање. Ови системи су нпр. у Руској Федерацији само делом доступни на мрежи (други део је потпуно изолован), док су у USA и UK, ови системи повезани *on-line*, што неминовно повећава потенцијалне сајбер ризике [151].

Бројни експерти за сајбер безбедност сматрају да увођење **Wi-Fi** у **авион**, представља значајан **безбедносни ризик**, и да интернет конекција у путничкој кабини представља директну везу између авиона и спољашњег света, а што укључује и потенцијалне злонамерне учеснике. Тако, демонстрирано је (2013), да је могуће хаковати авион помоћу *android smartphone* [153]. Такође, показано је (2015) да је могуће ометати сателитске комуникације, а тако и навигационе системе за летење, користећи IFE, тј. системе за забаву путника. Наиме, *Chris Roberts,* стручњак из области сајбер безбедности, пријавио је FBI-у (USA *Federal Bureau of Investigation*) да је преко IFE авиона, који је био у лету, укуцавши команду ″CLB″ (пењање), накратко променио трајекторију авиона [154]. Свакако, најгори сценарио би био да терориста с лаптопом буде међу путницима и користећи Wi-Fi преузме контролу над авионом. Поред тога, испитивање сајбер безбедносних ризика ATM/ATC система показала је нпр. да постоје значајне слабости ATM система FAA, и оне се кључно односе на процедуре за контролу приступа и могућности идентификације незаконитих ″упада″, тј. неовлашћеног приступа рачунарским системима (идентификација и ауторизација корисника, енкрипција осетљивих података, ревизија и праћење активности на системима FAA, итд.) [155]. Сматра се да су неке од ових слабости узроковане недостатком свеобухватне стратегије за управљање сајбер ризицима, односно недостатком прецизно дефинисаних улога и одговорности у оквиру FAA.

Које су **критичне тачке** авио система, које могу бити потенцијално нападнуте од стране појединаца (хакер/сајбер терориста), корпорација или држава, због чега је савремени авио систем нарочито изложен сајбер нападима, и које су кључне претње? Бројне су слабе/критичне тачке – мете авио система, а потенцијалне су: индустрије за производњу авиона и авио компонената, електронски системи компанија за дизајнирање хардвера и софтвера које користе аеродроми, као и системи контроле летења. Навешћемо укратко следеће чињенице у вези са **сајбер рањивостима** авио система (контрола летења, авион, авио компаније, аеродроми и пограничне власти).

- **Контрола летења** (ATC): повећање аутоматизације ATC, као и употребе беспилотних летилица (*Unmanned Aerial Systems,* UAS, односно дронова (фуснота 113), што подразумева коришћење интернет комуникације између земаљских контролних станица и ваздухоплова, излаже ATC новим рањивостима. Како сајбер стручњаци истичу, ATC систем је веома подложан сајбер нападима, и то нарочито ADS–B систем, који није енкриптован и аутентификован у довољној мери, тако да се може неовлашћено прислушкивати и оштетити коришћењем ″паметних″ телефона (део 3.1.2.1).
- **Авион**: најновија решења, која се уводе у авио системе, као COTS (фуснота 52) софтверска и хардверска готова решења, значајно повећавају сајбер ризике. Затим, ризик од сајбер напада представља повезивање система за комуникацију свих рутинских команди авиона и ATC, као и повећање размене порука при комуникацији с авионом, што повећава потенцијалну рањивост авиона. Нарочито, novi *e-Enabled* авиони, затим, ATM системи дизајнирани од стране SESAR (*Single European Sky* ATM *Research*), као и NextGen (*Next Generation Air Transportation System*) и CARATS (*Civil Aviation Reform of Air Traffic Services*)

пројекти [156], већ су у употреби, при чему, интерповезани, међусобно зависни системи авиона, повећавају сајбер рањивости (део 3.1.2.2). Тако, иако је *"Connexion by Boeing"* напуштен[64], авио индустрија ради на налажењу нових решења за *on-board* интернет повезивање, а то може увести нове сајбер ризике и изазове.

- **Авио компаније**: рањивости су *web* апликације, као нпр. *Sykipot backdoor tool* који прикупља обавештајне информације или експлоатација *Twitter* налога, што може нанети штету авио компанијама (део 3.1.2.3).
- **Аеродроми и пограничне власти**: због свеприсутног повезивања аеродрома, преко интернета, као и екстерних мрежа, потенцијалне мете сајбер напада су класична информационо-технолошка структура аеродрома, као и унутрашње аеродромске операције (део 3.1.2.4). Фокус је на обезбеђивању система контроле приступа и упада у периметар, *e-Enabled* авионских система, радарских система, бежичних и жичаних мрежних система и мрежних система за пртљаг. При томе, морају се узети у обзир и интегрисати основни принципи безбедности (поверљивост, интегритет, доступност и веродостојност).

3.1.2.1. Контрола летења

Контрола летења (ATC) је комплексан систем, који функционише у складу с националним и међународним законодавством, а чији се рад заснива на процедурама, организацији и технолошким инструментима, у циљу спречавања колизије између авиона и/или између авиона и других "препрека", затим, организовања и безбедног протока ваздушног саобраћаја, пружања информација и препорука пилотима за ефикасно и квалитетно обављање летачке операције, као и пружања информација трећим лицима у операцијама спашавања/трагања. У већини држава, ATC пружа услуге свима, приватним, војним, комерцијалним и државним превозницима, који послују у оквиру својих ваздушних простора, а у зависности од врсте лета и класе ваздушног простора, ATC даје препоруке које пилоти могу/не морају следити, или упутства која пилоти морају следити, с изузетком јасно уочених хитних случајева[65].

ATC (контрола на земљи, локална контрола и контрола подручја) сервисира све фазе кретања авиона. Земаљска контрола, координирана с контролног торња аеродрома, регулише и организује кретање ваздухоплова и других возила у зони аеродрома, укључујући улазак у/сизлазак са рулне стазе, неактивне полетно/слетне стазе (писте), зоне заустављања и транзита (у одласку, након напуштања *gate*-а, по доласку и силаска с писте). *Ground Control*, координисана са контролног торња аеродрома, регулише и организује маневрисање ваздухоплова на земаљским површинама, као и других возила у зони аеродрома, укључујући улазак у/сизлазак са рулне стазе, неактивне писте, зоне заустављања и транзита (у одласку до писте,

---

[64] *"Connexion by Boeing"* био је бежични сервис за пружање Wi-Fi услуга у авионима компаније *Boeing*, осмишљен и промовисан заједнички од стране *Intel*-а и *Boing*-а; омогућавао је да власници *Centrino* лаптопова користе *wireless* могућности својих рачунара за повезивање на интернет и када су у авиону. Међутим, евидентирани су ризици код употребе овог сервиса, као и да исти може изазвати проблеме у раду електронских система у авиону.

[65] За безбедност авиона, одговоран је пилот [157].

по доласку након напуштања писте). Сваки ваздухоплов/возило/особа која се креће у овим контролисаним областима мора добити изричито овлашћење од земаљске контроле путем VHF/UHF фреквенције. Локална контрола, којим управља контролни торањ, одговорна је за коришћење писте (*runway,* RWY), рулне стазе до RWY, фазе полетања/слетања авиона (*Approach Control*), за које даје посебна одобрења и упутства, обезбеђујући раздвајање између ваздухоплова у сваком тренутку. У фази пре полетања, локална контрола даје пилоту индикације за рулну стазу и полетно-слетну стазу и упутства за руту по полетању, уз одговарајућа овлашћења (*Clearance Delivery*). *Flight Data,* добијени са *Clearance Delivery,* је ресурс који пилотима даје тачне и ажуриране информације о временским варијацијама, прекидима, кашњењима у операцијама на земљи, затварању писте, итд. и који се емитују у непрекидној петљи преко наменске фреквенције *Automatic Terminal Information Service* (ATIS). У случају аномалија у авиону који је у фази слетања, локална контрола може издати директиву за обилазак, дајући инструкцију пилоту да прекине операције слетања и да буде спреман да прими нова упутства. Контрола подручја обезбеђује *Area Control Centres* (ACC), тј. ACC-у додељен FIR (*flight information region*) у коме се авион налази током фазе крстарења. Основне ATC услуге за сваки FIR састоје се из *Flight Information Service* (FIS) и *Alerting Service* (ALS). Подаци FIS-а обухватају метеоролошке услове, вулканску активност, присуство радиоактивних или токсичних супстанци у атмосфери, промене у оперативној ефикасности навигационих уређаја, беспилотне летилице, ризик од судара и свих других безбедносних информација; ALS обавештава надлежне органе о авионима којима су потребне операције потраге и спасавања, и помаже им по потреби.

Дакле, ATC обухвата различите системе (системи контроле, комуникације и надзора), који се користе у различитим фазама контроле ваздушног саобраћаја.

Flight Data Processing (**FDP**) је ATC систем, који анализира податке планова лета у различите сврхе, затим, даје контролорима ваздушног саобраћаја широк спектар информација о плану лета, као и 30–60 минутну метеоролошку прогнозу ваздушних саобраћајних услова, што омогућава да се предупреде потенцијално опасне ситуације и донесу ефикасне одлуке о планирању ваздушног саобраћаја.

Control Working Position (**CWP**) је контролна станица ваздушног саобраћаја, тј. ATC систем, који интегрише бројне системе неопходне за рад контролора: радарске екране, ваздухопловне и географске карте, метеоролошке услове, саобраћај на земљи (аеродрому), комуникационе системе, и системе за предвиђање могућих средњих и кратких трајекторија лета. На мониторима CWP приказују се тренутни услови ваздушног саобраћаја, добијени интеграцијом података које емитује радарски систем и FDP.

Air Navigation Service Provider (**ANSP**) је правни/приватни субјект, који управља ваздушним саобраћајем у име компаније/региона/државе, и то нарочито усмерен на земаљске телекомуникације. ANSP телекомуникациона конективност постиже се новом интегрисаном оперативном комуникационом мрежом – *E-Net,* чија имплементација има за циљ повезивање ACC-е, аеродроме, контролне торње и радарске центре преко телекомуникационог система модулираног према локацији

и услузи. Крајњи циљ овог начина конекције је повећање поузданости и успешности комуникације на различитим нивоима.

Controller Pilot Data-Link Communication (**CPDLC**) је систем који омогућава размену дигиталних порука. Авион је опремљен пријемником/предајником којим се остварује комуникација између пилота и АТС (земаљска контрола) коришћењем аналогног система који ради на VHF/UHV фреквенцијама. У циљу ефикасније комуникације, препорука је коришћење CPDLC.

ARTAS (ATM *Surveillance Tracker and Server*), дизајниран од стране EUROCONTROL-а, јесте систем[66] који омогућава добијање прецизне слике "ситуације у ваздуху", тј. података у прецизно дефинисаном географском подручју, као и дистрибуцију тих података. Поред тога, ATIS као аутоматизован систем, који користи наменску фреквенцију или се може повезати са VOR предајником, даје пилотима континуиране метеоролошке и оперативне податке, а који се односе на одређени аеродром. Такође, *Satellite Distribution System* (SADIS) јесте сателитски систем, који даје и ажурира информације и слике високе резолуције у вези с метеоролошким условима.

ATM системи цивилног ваздухопловства суочавају се с дугим процесом трансформације, који отвара веома важна питања у вези с њиховом сајбер безбедношћу. У циљу модернизације ваздушног саобраћаја и побољшања слања/примања дигиталних информација, тј. *data link* комуникације, FAA у USA и EUROCONTROL у Европи, уводе NextGen и SESAR пројекте у вези са управљањем ваздушним саобраћајем. Европске и америчке власти постигле су прелиминарни споразум (2010) о интероперабилности њихових будућих система за управљање ваздушним саобраћајем, SESAR и NextGen [158].

Имплементација **NextGen**-а, као новог система контроле ваздушног саобраћаја USA, почела је 2012. године, у фазама. С обзиром на процене FAA, нерешавање проблема "загушења" у авио систему USA изазваће огромне финансијске губитке у времену које долази [158]. Пројекат *NextGen* обезбеђује превазилажење ових проблема – нова опрема авиона омогућава авионима да безбедно лете на мањем међусобном растојању, повећавајући обим и дистрибуцију информација, што резултује у повећању ефикасности авио операција и аеродрома (брже слетање авиона, боље предикције метеоролошких услова, аутоматизације и дељења информација, смањење времена за таксирање, итд.). Као резултат тога, смањује се потрошње горива и емисије штетних гасова, као и времена и миља проведених у ваздуху. ***Single European Sky***[67] – Јединствено европско небо, заједнички пројекат држава чланица европске уније, чији је циљ суштинско редефинисање европског

[66] Радарска контрола ваздушног саобраћаја комбинује податке различитих радарских сензора, који се дезинтегришу специфичним системима, и након тога су доступни контролорима. Овај сектор се убрзано развија, а ARTAS и слични системи су резултат напретка у овом сектору.

[67] Непосредни повод за покретање овог пројекта за ваздухопловни саобраћај, је ерупција вулкана Ејафјадлајекидл (Исланд, 2010). Последица ове изненадне ерупције, био је највећи застој авио саобраћаја у историји ваздухопловства. Због тога су министри саобраћаја држава чланица EU, као најзначајнији приоритет, поставили успостављање јединственог европског неба, у циљу спречавања неког будућег хаоса у ваздушном саобраћају.

ваздушног простора и ATM-а. Развој потребног технолошког капацитета омогућен је дизајнирањем SESAR програма (2004), чија је имплементација започела 2014. године. Најважнији циљеви SESAR-а су: динамички план рада мреже, потпуна интеграција аеродромских операција у оквиру ATM и процеса планирања, нови начини раздвајања авиона, затим, повезивање свих учесника ATM који ће делити исте податке, као и увођење нових аутоматских функција као помоћ пилотима и контролорима (смањење обима посла у циљу лакшег доношења одлука). Реализацији програма SESAR потенцијално може довести до губитка контроле над војним ваздушним операцијама, због чега владе неких држава не подржавају овај програм. Томе у прилог иде и чињеница да развој регионалних мрежа за управљање авио саобраћајем доводи до смањења броја радних места. Такође, до значајног угрожавања пословања европских оператера долази и због нелегалних летова, што има и негативан утицај на општу безбедност европског неба. Због тога, оператери и регулаторне агенције заједнички раде на проналажењу решења за спречавање/санкционисање оператера који игноришу или заобилазе прописана правила и регулативе.

Дакле, пројекти NextGen и *Single European Sky*, представљају еволуцију ATC базиране на системима на земљи (*ground-based system*) у ону засновану на сателитским системима управљања већим бројем комуникационих веза и услуга [159]. Међутим, као што је и поменуто, нове технологије отварају нове **безбедносне ризике**, због тога што омогућавају већу размену информација, и то не само између ATC и авиона, већ и између других ентитета и актера – прелазак са једног начина комуникације на други, повећава број рањивости, које могу искористити сајбер преступници. На пример, поменути ADS–B је био главна мета напада за етичке хакере групе *white-hat*[68]. Они су показали како се са опремом од 2.000 $, може увести ″авион – дух″ на екран контролора летења, захваљујући томе што није постојао процес утврђивања места доласка порука, као и процес провере аутентичности података. Исте године, *Teso Hugo*, професионални пилот и истраживач, показао је на *DerbyCon* конференцији у Амстердаму (2013), да је могуће хаковати авион коришћењем *Android Smartphone* [153]. Међутим, FAA и EASA, накнадно су указале на ограничену валидност теста, као и да Тесов метод не даје исти резултат уколико се користе софтверске апликације инсталиране на сертификованој опреми авиона.

Авио индустрија, може бити изложена **сајбер безбедносним претњама**, краткоточно и дугорочно. Развијене државе запада, као што су USA и UK, издвајају велика материјална средства у образовање ICT стручњака, а основни приоритет на националном ниво је онемогућавање да ови, висококвалификовани ICT стручњаци постану симпатизери/чланови криминалних или терористичких група. У вези са тим, IT стручњак *Junaid Hussain*, који је према америчким изворима, консолидовао и институционализовао интересе ISIS-а у сфери сајбер напада (претпоставља се да је, пре него што је убијен 2015. године, подучавао регруте ISIS-а техникама

[68] W*hite-hat* – односи се на етичко хаковање, тј. добронамерне хакере, специјализоване за тестирање пенетрације и других метода, које омогућавају безбедност организационих информационих система; супротно од овога је *black-hat*, који се односи на злонамерне хакере (део 2.1.1.2).

хаковања) је само појединачни случај на нивоу екцеса [146]. Овај инцидент је, на неко време, успорио технолошку еволуцију терористичких организација, али је предикција да ће се сајбер преступници технички усавршавати, као и да ће се организовани криминал све више ослањати на хакере за своје илегалне активности. Уколико се такав тренд настави, сајбер претње ће бити озбиљније, због пораста броја међусобно конектованих уређаја и све веће конкуренције на тржишту *malwere*-а. Могуће је и да сајбер криминалци добију приступ високо софистицираним инструментима, али се претпоставља и да ће опасност, коју ови актери представљају за систем ваздушног саобраћаја, остати на релативно ниском нивоу у времену које долази [146].

3.1.2.2. Авион

Авион је софистицирани инжењерски систем. Састоји се од **комплексне мреже компоненти**, које укључују комуникационе везе, сензоре и електронске системе авиона[69], као нпр. *Flight Managment System* (FMS), *glass cocpit/flight display*, *Traffic Alert and Collision Avoidance System* (TCAS), *Airborne Collision Avoidance System* (ACAS) и *Aircraft Communications, Addressing and Reporting System* (ACARS). Као и сваки рачунар, ове компоненте и комуникационе мреже, изложене су различитим врстама сајбер напада (нпр. ометање и лажирање, део 2.1.1.2).

У авионским мрежама, користе се етернет (фуснота 24) мреже, као што је *Avionics Full DupleX Switched Ethernet* (AFDX)[70]. Жичане комуникације обезбеђују безбеднију мрежу с високим степеном поузданости, с обзиром на то да им је теже приступити [161]. С друге стране, *Avionics Wireless Network* (AWN) представља нове изазове у вези са тачношћу, поузданошћу и безбедношћу [162]. **Авионика**, осим што укључује IFE системе за забаву путника (део 3.1.1), обезбеђује и контролне летачке функције, навигације, навођења, комуникације и мониторинга. Висок ниво интеграције доводи до забринутости у вези са сајбер безбедношћу, као нпр. код коришћења *Voice-over-the-Radio* (VoR) комуникације [163]. Главни недостаци **VoR** су временско кашњење пријема сигнала, нарочито у случају вишеструких комуникација, и нејасноће у комуникацији између контролора и пилота, услед шума. С друге стране, **CPDLC** [164] је дигиталан и стога отпорнији. Поред ових комуникационих протокола, користе се и други, као што је **ACARS** [165], који ће бити описан у наставку текста, као и потенцијалне сајбер претње у различитим комуникационим протоколима ваздух–земља [149]. Најскорије, ваздухопловна заједница се фокусира на стварање модерног *United States National Airspace System* (NAS) подржаног новим комуникационим системом који може побољшати интеракцију између авиона и система на земљи [159].

---

[69] Електронски системи авиона (авионика) су системи широког спектра функционалности, који укључују комуникације, навигацију, дисплеј, надзор, одржавање, радар, ажурирања у вези с временским условима, итд. Дакле, авионика се дефинише као комбинација авио-система и електронике, који се састоји од уграђених система у пројектовању, развоју и експлоатацији авиона [160].

[70] AFDX је IEEE 802.11 протокол базиран на WFMS-у (*Wireless Flight Management System*).

Детаљније о различитим компонентама авиона/авионике, а које могу бити изложене сајбер нападима, дато је у наставку текста.

Flight Managment System (**FMS**) је веома важан део авио-електронских система, који подржава бројне активности/задатке током лета авиона, обезбеђујући информационе функције као што су оне у вези с навигацијом, планирањем лета, предвиђањем трајекторије, прорачуном перформанси и навођење током лета. За имплементирање ових функција (које, због важности FMS-а за безбедно фукционисање авиона, морају бити високо поуздане и отпорне на грешке), неопходно је повезивање FMS-а с другим системима авионике. Иако се специфичне имплементације FMS-а могу разликовати, овај систем генерално се састоји од рачунарске јединице (обезбеђује ресурсе за све компјутерске прорачуне и успостављање интерфејса с другим авио системима; за FMS -ове, с мањим скупом функционалности, може се реализовати као нестандардна самостална јединица, док за веће FMS-ове, рачунарска јединица често захтева коришћење снажнијих процесора, као што је *Integrated Modular Avionics* [166] и јединице контролног дисплеја (примарни интерфејс за пилоте, који се користи за унос података, као и приказ информација добијених од FMS-а).

Glass cocpit је пилотска кабина у којој се подаци о лету приказују на *Electronic Flight Displays* (EFDs), а не на одвојеним, самосталним екранима за представљање резултата релевантног мерења[71]. EFDs, тј. *Electronic Flight Instrument System* (EFIS) (сл. 4) су *Primary Flight Display* (PFD), који комбинује податке из неколико инструмената и који је пилотов примарни извор информација о лету, и *Multi-Function Display* (MFD), који омогућава приказивање података на више страница, а које се на једноставан начин, по потреби, могу мењати.

Бенефити *Glass cocpit*-а су:

- Једноставније очитавање вредности, без паралаксе (очитавање не зависи од угла под којим особа гледа у инструмент), као и јаснији приказ због употребе прецизних нумеричких вредности (за разлику од аналогног дисплеја); ово омогућава пилотима свеубохватније и брже сагледавање укупне ситуације.
- Омогућава представљање различитих нивоа информација (сл. 4. б и в), што је нарочито корисно за различите приказе, нпр. метеоролошких услова, орографије, терена, државних граница, ваздушног простора и других авиона у ваздуху, што драстично смањују ризике од "уласка" у олује, *Controlled Flight Into Terrain* (**CFIT**)[72], повреду ваздушног простора, губитак раздвајања авиона, итд.

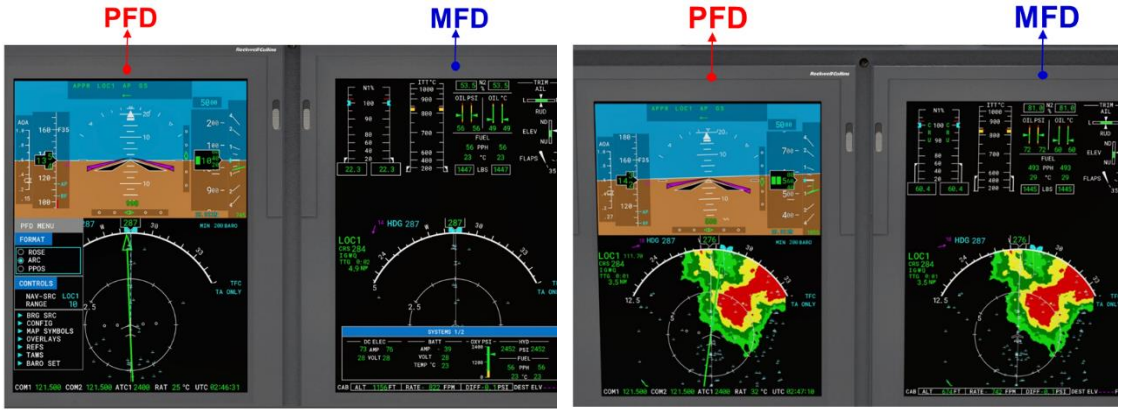
[71] Код традиционално коришћених авио-инструмената, свака променљива приказана у кокпиту има наменски подсистем инструмента с припадајућим дисплејом.

[72] CFIT се дефинише као ненамерни судар с тереном (тло, планина, вода или препрека) док је авион у потпуности под контролом (без отказа авио система). Већина CFIT се дешава у фази приласка писти/слетања авиона, а пилот/посада нису свесни претеће катастрофе. Један од главних фактора CFIT је губитак свести о ситуацији – континуирано непознавање тренутне позиције авиона, тј. непрецизни прилази. Иако је број CFIT акцидената у последњих двадесет година драстично смањен, ипак се ове несреће и даље догађају, а најмање 50% њих је са фаталним исходом [167].

- Дисплеј заузима мање простора на инструмент-табли кокпита, а приказује више података и даје свеобухватније информације (сл. 4а), што помаже пилотима брже сагледавање свих података и бржу процену ситуације
- Електронски дисплеј је повезан с рачунаром, што омогућава обраду података из више извора; резултат тога је да се подаци представљају ергономскије, а упозорења су уочљивија.

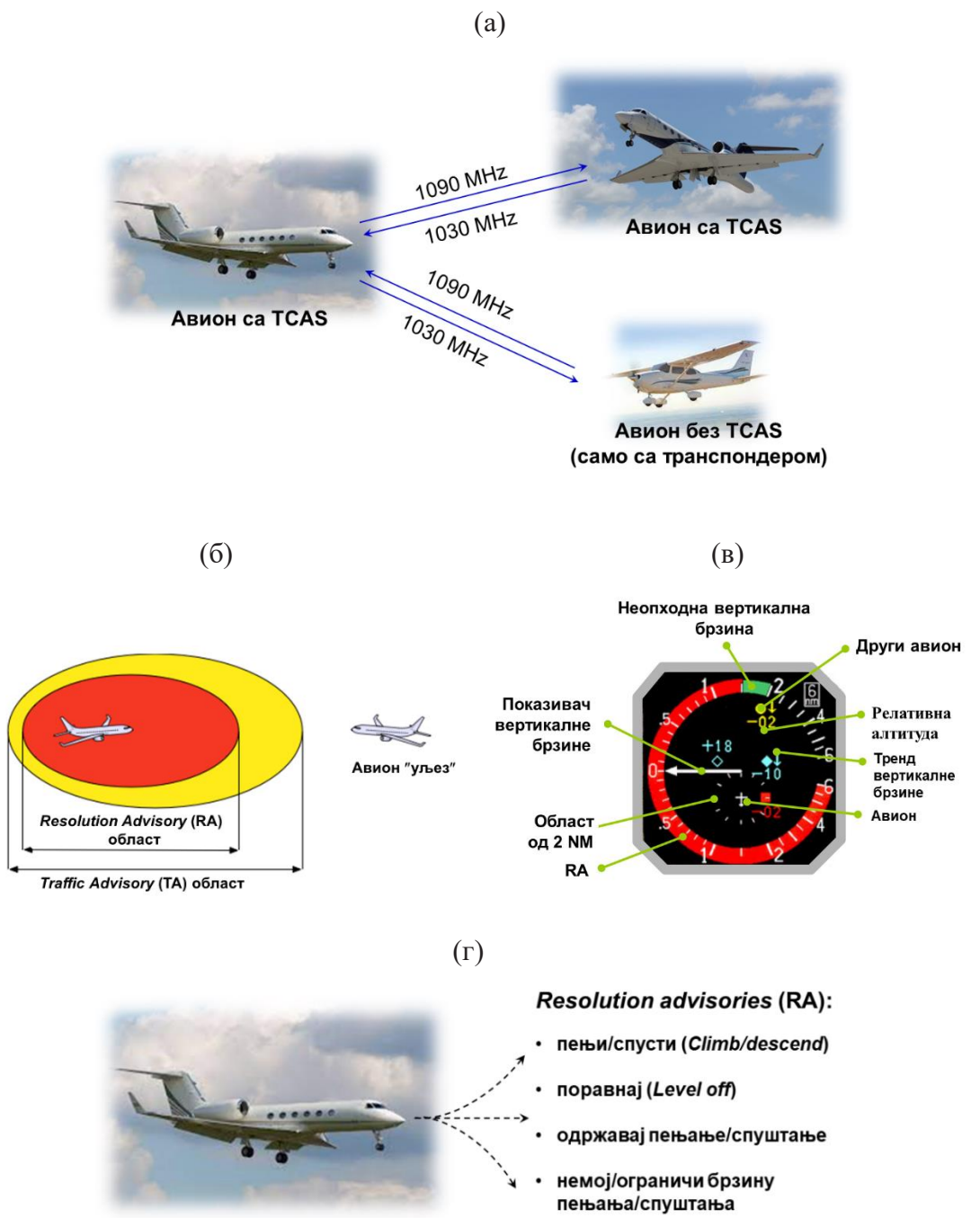
(а)

(б) (в)



Слика 4. Пример *Glass cocpit*-а са *Primary Flight Display* (PFD) и *Multi-Function Display* (MFD) (а) и различити нивои информација представљених на PFD и MFD (б и в) (преузето и модификовано из [170, 171 и 172])

Traffic Alert and Collision Avoidance System (**TCAS**) је бежични систем упозорења о саобраћају и избегавању судара, дизајниран на начин да се смањи учесталост судара с другим авионима, у ваздуху. Овај систем функционише независно од АТС и навигационих инструмената [168, 169]. Функционисање TCAS-а приказано је на сл. 5.



Слика 5. Најважнији елементи функционисања *Traffic Alert and Collision Avoidance System*-а (TCAS): (а) ваздушни надзор (*airborne surveillance*), (б) сигурносна логика (*safety logic*), (в) вертикално раздвајање (*vertical advisories*) и (г) интерфејс с пилотом (*pilot interface*) (модификовано и преузето из [168])

TCAS се састоји од четири основне компоненте (сл. 5): надзор током лета, сигурносна логика, вертикално раздвајање и интерфејс с пилотом. Уколико постоји потенцијална претња (још један авион у ваздуху), TCAS даје обавештење о саобраћају (*traffic advisory,* TA), тј. обавештава пилоте звучном најавом – "*Traffic, Traffic*", и наглашава позицију интрудера на дисплеју, у циљу помоћи пилотима у

уочавању другог/других авиона, као и за припрему пилота за потенцијални маневар избегавања. Уколико маневар постане неопходан, систем ће издати упозорење о решавању (*resolution advisory,* RA), наводећи пилоте да се пењу/спуштају како би задржали безбедну удаљеност. Постоји звучна најава потребног вертикалног маневра, а опсег прихватљивих вертикалних брзина је приказан на индикатору вертикалне брзине. TCAS може издати низ различитих савета (не пењи/не спуштај, ограничавање пењања/спуштања на 500, 1.000 или 2.000 ft/min, пењање/спуштање брзином од 1.500 ft/min, итд.). У зависности од ситуације, TCAS може ојачати, ослабити или променити смер инструкција, при чему упозорење о решавању, односи се искључиво на *vertical advisories*; TCAS не врши хоризонталне маневре као што су промене смера или скретања. Након што је ″сукоб″ решен, TCAS објављује *″Clear of Conflict″.* Одређивање тренутка упозорења и шта саветовати, представља бројна правила. Иако су генерални кораци које TCAS користи за избор савета релативно једноставни, детаљи логике веома су сложени. У TCAS логичку спецификацију уграђена су многа хеуристичка правила и подешавања параметара дизајнирана у циљу компензације шума и грешке сензора, као и варијабилности у одзиву пилота. Постоје и правила која регулишу када треба ојачати, ослабити и поништити савете, као и како поступати у ситуацији, у којој је више истоивремено присутних авиона ″уљеза″.

Побољшање TCAS-а представља *Airborne Collision Avoidance System* (**ACAS**), тј. систем за избегавање судара у ваздуху, који подржава надзор заснован на GPS подацима и користи нове моделе сензора (радарске и електро-оптичке), који су нарочито важни за беспилотне платформе. ACAS омогућава избегавања судара за нове класе корисника, укључујући мале авионе генералне авијације које тренутно нису опремљене TCAS-ом. ACAS је револуција у дефинисању и представљају *advisory logic* – уместо коришћења *ad-hoc* псеудокода заснованог на правилима, ACAS представља логику која користи нумеричку табелу оптимизовану према моделима ваздушног простора. Овај нови приступ побољшава робустност, подржава нове захтеве и смањује непотребна упозорења, а његово усвајање значајно смањује трошкове имплементације и одржавања [173]. Дакле, ACAS се заснива на сигналима/одговорима транспондера SSR-а, који функционише независно од опреме на земљи, дајући информације пилотима о потенцијалним конфликтним ситуацијама, тј. другим авионима који су опремљени SSR транспондерима [148] Не могу се сви TCAS, сматрати прихваћеним ACAS. Тако, TCAS I је обавезан у USA за мање авионе, а у Европи, обавезни су TCAS II верзије 7.0 и 7.1, а које су тренутно једине комерцијално доступне имплементације ICAO стандарда за ACAS II. ACAS II је систем, који се заснива на сигналима транспондера SSR-а; шање упите транспондерима *Mode* C и *Mode* S авиона у околини (″уљез″) и из одговора прати њихову алтитуду и домет, као и издаје упозорења пилотима, према потреби. ACAS II ради независно од навигације авиона, система управљања летом и ATC.

Поред могућности вербалне комуникације, авиони најчешће поседују *Aircraft Communications, Addressing and Reporting System* (**ACARS**). Овај систем се користи за слање дигиталних порука у оба смера, авионима, авио компанијама и другим ентитетима авио система, и уведен је у циљу смањења оптерећења посаде и

повећања интегритета података. ACARS систем састоји се од јединице контролног дисплеја (*Control Display Unit*, CDU) и управљачке јединице (ACARS *Management Unit*, MU). ACARS MU шаље и прима дигиталне поруке са земље користећи VHF радио-фреквенције; на земљи, систем – мрежа радио примопредајника, прима и емитује *data link* поруке, као и усмерава их на различите авионе, који су на мрежи. ACARS систем не поседују мањи авиони, који се користе у приватној авијацији. Међутим, ови авиони опремљени су транспордерима – електронским уређајима, који комбинују способност преношења информација и добијања одговора на упите с радара АТС. При томе, највећи део ове комуникације је аутоматизован. Помоћу транспордера, АТС добија информације о локацији авиона у ваздушном простору и висини (*altitude*), што омогућава АТС-у безбедно и сигурно регулисање авио саобраћаја. Употреба ACARS, осим првобитне намене, проширена је на операције спашавања/трагања и аутоматизованог мерења времена лета, тј. посаде. Тако, осим што ACARS систематски нарушава приватност локације, подрива и приватност корисника, јер су осетљиве информације пренете преко ACARS бежичног канала, подложне нападима прислушкивања [149, 174].

Типични представници нових технологија, који омогућавају употребу и обједињавање различитих апликација из домена управљања ваздушним саобраћајем су транспондер, ADS–B и *Head-up display* (HUD).

Транспондер (XPDR, XPNDR, TPDR или TP) је пријемник/предајник у авиону, који генерише одговор, тј. сигнал, након одређеног упита; одговор и упит су на различитим фреквенцијама (додељује ICAO). Сваком ваздухоплову који лети у контролисаном ваздушном простору, додељује се посебан код транспондера[73] (у авијацији се најчешће користи реч "*squawk*" за SSR кôд) [175], како би га АТС оператор једноставно идентификовао на екрану радара, користећи SSR. Транспордери, којима се опремају авиони, могу бити различитог режима рада, тј. мода[74]: *Mode* A (шаље идентификациони код), *Mode* C (омогућава АТС оператеру аутоматско очитавање висине и нивоа лета – FL-*Flight Level* на коме се налази упитани авион) и *Mode* S (укључује и *Mode* A и *Mode* C), који даје аутоматску идентификацију и податке о висини ваздухоплова, као и статусу лета); транспондери C и S мода, обавезна су опрема у већини прометних зона контролисаног ваздушног простора. У АТМ-у, транспондери се користе у различите сврхе, као нпр. за идентификацију авиона, повећање свесности ситуације и развој АТС алата и сигурносних мрежа, као што су AMAN (*Arrival Manager*), MTCD (*Medium-Term Conflict Detection*), STCA (*Short-Term Conflict Alert*), итд.

---

[73] Транспондерски кôд (састоји се од четири цифре, односно 4.096 различитих комбинација цифара од 0 до 7), селектује пилот, на основу кôда који је АТС доделила пилоту; кôд (стандардни) 1200, користи се уколико пилот лети према *Visual Flight Rules* (VFR). У хитним случајевима користе се следећи кодови: 7500 (отмица), 7600 (губитак комуникације) и 7700 (општа опасност). Детаљи у вези са стандардним кодовима у различитим државама дати су у националним *Aeronautical Information Publications* (AIPs).

[74] Примо-предајник (Tx/Rx-*Transmiter*/*Receiver*) на земљи назива се интерогатор и чине га Tx (функционише на 1030 MHz) и Rx (функционише на 1090 MHz). Интерогатор шаље у етар питања у облику електронске шифре, а из авиона добија одговор само оних авиона који имају транспондер/упитну шифру одређеног мода/кода (мод је временски интервал између два пара импулса, док је кôд комбинација међусигнала између два пара импулса.

Претходно описани системи, ACAS и TCAS, захтевају да и авион–упит и авион–циљ буду опремљени оперативним транспондерима. При томе, авион опремљен ACAS/TCAS-ом добија одређене информације у зависности од врсте транспондера којим је опремљен авион–циљ. И неки други системи [176], као што су *Airport Surface Detection Equipment–Model* X и *Advanced Surface Movement Guidance and Control System* употребљавају транспондере у циљу повећања оперативне безбедности и сигурности.

Automatic Dependent Surveillance – Broadcast (**ADS–B**) је веома важан систем, настао као потреба за осматрањем ваздушних области без радарске покривености и оптимизацијом раздвајања ваздухоплова, тј. за ефикасним решавањем различитих питања, која су у вези с капацитетом ваздушног простора [177, 178]. Ова савремена технологија, која обједињује позната техничка решења из области телекоминикације, навигације и осматрања ваздушног простора, саставни је део FAA пројекта NextGen и EUROCONTROL CASCADE програма, и представља еволуцију земаљске контроле ваздушног саобраћаја у ону засновану на сателитским контролним системима с бројним комуникационим везама и услугама, у циљу повећања побољшања безбедности, економичности, аутоматизације, екологије и сл. Основе ADS–B (инфраструктура, рад и ограничења) биће дате у посебном делу дисертације (глава 6), за лакше разумевање безбедносних проблема и ограничења протокола, као и сагледавање различитих начина на које ADS–B може бити потенцијално нападнут, и последично угрозити безбедност ваздухопловства у свим њеним аспектима. Како је саставни део ADS–B система, а који функционише самостално и аутоматизовано доставља неопходне податке корисницима, како на земљи, тако и у ваздуху, GNSS систем, овај систем ће бити детаљније описан у глави 5.

У циљу повећања безбедности авио операција током полетања и слетања [179, 180], *Global Aviation Safety Road Map*, даје препоруку употребе **HUD** (*Head-up display*)[75] технологије [181]. HUD, први пут примењен у цивилној авијацији 1993. године, јесте јединствен концепт, који пројектовањем критичних података/информација о лету на HUD (у нивоу очију пилота), омогућава пилотима визуелизацију одређених ситуација изван кокпита, и сагледавање симболима приказане параметре, као што су смер ваздушних струја и висину, смер, курс и путању лета (сл. 6). На овај начин, смањује се оптерећење пилота, повећава свесност ситуације, као и омогућава прецизније слетање и полетање, што може смањити број потенцијалних авио несрећа[76].

HUD се састоји од: (а) рачунара (прима податке у реалном времену и генерише симболичке приказе; (б) јединице за пројектовање оперативних података; (в) екрана, тзв. комбинатора (транспарентни екран, који се налази испред пилота и представља ″холографски оптички елемент″, направљен од стакла или пластике);

[75] Назив за HUD је и *Enhanced Flight Vision System* (EFVS).

[76] Значајна анализа, спроведена од стране *Flight Safety Foundation*, показала је да би употреба HUD могла да спречи/ублажи 38% авионских несрећа током периода од 13 година [182].

(г) контролног панела (омогућава пилоту да изабере неку од опција приказа/уноса података).

Слика 6. Транспаретни приказ најновије технологије HUD (*Head-up display*) система за *Boeing* B737 са подацима (преузето и модификовано из [185])

Веома важан аспект употребе HUD-а је људски фактор (разумевање људског понашања и учинка), који се у авијацији најчешће односи на аспекте људске грешке у авио несрећама и кваровима система. Овде, "људски фактори" представљају специфичне елементе људског капацитета и факторе учинка као што је визуелна перцепција. Узимањем у обзир "дизајн усмерен на човека", тј. промишљено дизајнирање опреме и квалитетних компонената, смањују утицај људског фактора, као параметра који доприноси лошим перформансама и авио несрећама. За људе, очи (и центри за визуелну обраду и повезани оптички систем људског мозга) најважнији су извор информација, које се користе за процену и разумевање света око нас. Људска визија је покренула велики део еволуције технологије кокпита. За разлику од ранијих компликованих система, електронски прикази летења данашњих модерних авиона, сведочанство су напретка у инжењерингу људских фактора. Међутим, један од изазова у вези с људским факторима јесте чињеница да фокусирање на одређене појаве из окружења/информације омета фокус на друге, што може довести до "*attentional blindness*", тј. поремећаја пажње. Ова селективност је кључна за способност човека да функционише у сложеним окружењима, али такође може бити и потенцијална опасност – за ефикасно процесирање информација из различитих извора и правилно балансирање времена између фокусиране и подељене пажње, пилоти се подучавају процесу "скенирања" или кратког прегледа/посете сваког извора информација, узастопно на систематски начин [183]. Управо ово омогућава HUD дисплеј – преклапањем визуелних информација на спољашње окружење, олакшава истовремену обраду обе врсте визуелних инпута [184].

Нарочита предност коришћења HUD система јесте повећање свесности ситуације, нарочито ноћу, при ограниченој видљивости или лошим метеоролошким саобраћајним условима – дајући пилотима критичне податке лета, HUD омогућава прецизније и сигурније полетање/слетање у условима смањене видљивости и другим критичним ситуацијама, као и спречавање могућих CFIT (фуснота 72) акцидената при слетању. Ове безбедносне предности HUD, умногоме надмашују потенцијалне проблеме, а који су превазиђени током њихове употребе. Ови проблеми односили су се на поменуту усмерену пажњу (тзв. тунеловање) пилота, тј. губитак укупне свесности ситуације (јер пилот усмерава пажњу на HUD екран), као и на механичке недостатке (код раније генерације HUD). Решења за оба проблема, била су поједностављивање приказа информација, као и компоненти HUD уређаја. Ипак, ове проблеме је важно познавати и анализирати у специфичној обуци летачке посаде.

Предходно поменути системи и њихови кратки описи, дати су као помоћ за разумевање безбедносних проблема и различитих врста потенцијалних сајбер напада на авион, а тако и на безбедност ваздухопловства у свим њеним аспектима.

Сајбер безбедност ваздухоплова може се дефинисати као превенција и/или реакција на намерне злонамерне радње предузете путем сајбер средстава у циљу директног угрожавања система ваздухоплова, као и индиректног угрожавања авио система, онде где исти имају кључну улогу у ширем авио систему.

Раније, неколико инцидената је показало да је GPS био предмет намерног и ненамерног ометања од стране државних и недржавних актера. Тако, један од најконтроверзнијих сајбер инцидената, јесте **обарање беспилотне летилице** (RQ 170 *Sentinel*) у Ирану (2011), како се претпоставља, од стране јединице за сајбер ратовање иранских оружаних снага [146].

Такође, мистериозни **нестанак малезијског авиона** *Boeing* 777-200ER (MH370) са 227 путника и 12 чланова посаде (2014), отворио је питање тзв. сајбер-*jacking*-а, тј. отмице авиона употребом неконвенционалног сајбер оружја[77] [6]. "*Good night. Malaysian three seven zero"* – тако су отишле и последње речи са лета MH370. Три минута касније, авион је нестао са радарских екрана. Шта се заиста догодило са летом MH370 остаје једна од највећих мистерија у модерној авијацији, а бројни стручњаци покушавају да одговоре на кључно питање у вези с овом авио несрећом: како је могуће да модеран авион надзиран радарски и сателитски једноставно нестане? Чињеница је да је мистериозни нестанак лета MH370 открио слабости у системима ваздушне навигације глобално, као и да је увођење модерног система за надзор, тј. ADS–B система (описан у делу 6), неопходност. Детаљније, о нестанку MH370 (чињеницама, потрази и могућим узроцима несреће) дато је у делу 7.

Наведени примери су само врх леденог брега. У ваздухопловству, свака иновација у ITC, отвара нове могућности за сајбер напад и мора бити тестирана на

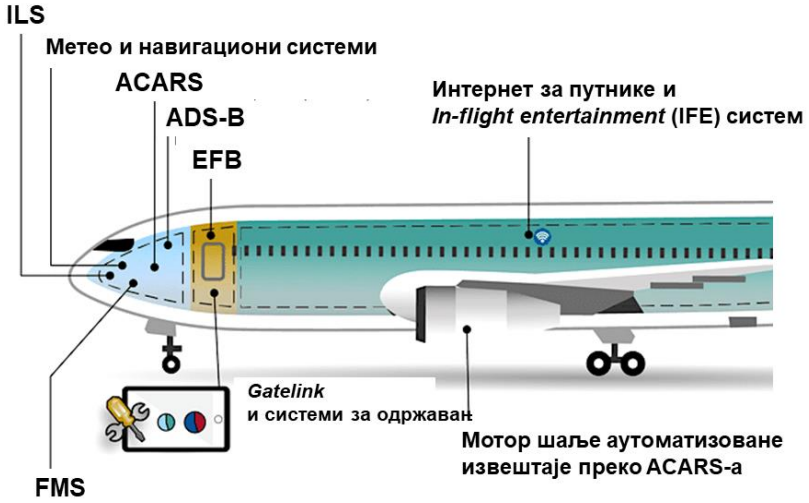
[77] Сајбер оружје представља „софтвер, фирмвер или хардвер, који је дизајниран или примењен да изазове штету кроз сајбер простор [186].

рањивост. Тако, авиони се све више ослањају на сложени софтвер који може имати безбедносне пропусте, а које могу искористити актери с криминалним намерама.

Осим потенцијалног фаталног исхода, тј. губитка људских живота, као и огромне материјалне штете, евидентан је и велики социо-психолошки ефекат оваквих напада, као што је било након серије координисаних терористичких напада, 11. септембра 2001. године против USA, познатих као **напади 9/11** (фуснота 45). Ови напади представљају серију отмица авиона и самоубилачке нападе 19 терориста повезаних с исламиском екстремистичком организацијом *al-Qaeda*, предузетих против циљева у USA, с највећим људским и материјалним губицима у америчкој историји – 2.750 људи у Њујорку, 184 особа у Пентагону и 40 људи у Пенсилванији, изгубило је живот. Полиција и ватрогасци у Њујорку били су нарочито погођени у нападима, а више од 400 полицајаца и ватрогасаца изгубило је живот [187].

Напади 9/11, трансформисали су безбедносна питања у авијацији, и веома брзо након њих, усвојене су драстичне и ригорозне безбедносне мере. Тако, основане су две велике организације – *Depatment of Homeland Security* (DHS) и *Transportation Security Administration* (TSA), и уведене бројне безбедносне мере, као што су инсталирање нових уређаја за проверу пртљага, ојачавање и закључавање врата кокпита, присуство мершалера на бројним летовима, ригорозније провере запослених, итд.

Савремени комерцијални авиони опремљени су мрежама и системима (сл. 7) који деле податке с летачким посадама, путницима, другим авионима, техничким особљем ангажованом на одржавању и контролорима летења, на начине који раније нису били могући.



Слика 7. Сајбер безбедносне претње на авион (преузето и модификовано из [188]) ILS – *Instrument Landing System*; ACARS – *Aircraft Communications, Addressing and Reporting System*; ADS–B – *Automatic Dependent Surveillance – Broadcast*; EFB – *Electronic Flight Bag*; FMS – *Flight Managment System*

Ова међусобна повезаност и зависност, може потенцијално довести до неовлашћеног даљинског приступа електронским системима авиона, као код поменутих, новијих типова (нпр. *Boing* 787 *Dreamliner* као и *Airbus* A350 и A380). Мета сајбер напада може бити цео авио систем авиона, или поједине компоненте система авиона. Поред тога, манипулацијама на авио систем, могу се извршити и физички напади на авион.

У авиону, вишеструке мреже за интерни и екстерни пренос података, омогућавају различите конекције између авионике и других система. Конекција ових мрежа зависи од техничких стандарда који се користе за њихову имплементацију. На пример, комерцијални авиони традиционално користе мреже које се ослањају на *Aeronautical Radio,* Inc. (ARINC) 429 стандард (развијен 1977. године). Напредније мреже обезбеђују ефикаснију, двосмерну комуникацију коришћењем новог стандарда AFDX (фуснота 70), развијеног 2005. године. Системи авионике користе ове напредне мреже за размену оперативних података с више система који се налазе изван авиона.

За **разумевање сајбер безбедности** [188] и **управљање сајбер ризиком** (део 4) ваздухопловна индустрија је дефинисала три концептуална домена:

- **Контролни домен ваздухоплова** (*aircraft control domain*) – најкритичнији домен, кога сачињавају системи и мреже чија је примарна функција подршка безбедним авио операцијама. Овај домен укључује авионику, све функције контроле летења, системе за управљање летом и навигацију, као и системе за безбедност путника (нпр. контрола животне средине и системи за детекцију дима). Системи у домену управљања авионом су одвојени од осталих система авиона.
- **Домен информационих услуга** (*airline information services domain*) – омогућава услуге и конекцију између других домена авиона, као што су контролни домен авиона, информације о путницима и услуге забаве, и било које *connected off-board networks*. Овај домен обухвата системе које користи посада авиона, укључујући и уређаје за управљање летом, тј. *electronic flight bags*' (EFB)[78], системе за праћење кварова, системе одржавања и аеродромске земаљске комуникације (неопходно је да буде изолована од домена путника). Поред тога, овај домен обезбеђује само ограничену количину података, преко једносмерног (или „само за читање“) канала путничком домену из домена контроле авиона, тако да путници могу да примају ажурирања статуса лета. Иако домен информационих услуга укључује податке који подржавају безбедан рад авиона, системи у оквиру овог домена немају могућност да издају команде које директно контролишу авион.
- **Домен информисања и забаве путника** (*domain of passenger information and entertainment*) – обухвата уређаје или функције које пружају услуге путницима,

[78] EFB је електронски уређај који користи летачка посада, и који приказује дигиталну документацију (навигационе карте, оперативне приручнике и контролне листе). EFB може вршити основне прорачуне планирања лета, а најнапреднији (приказују позицију авиона на навигационим картама, временске услове у реалном времену и обављају бројне сложене задатке планирања лета) укључени су у сертификоване авио-електронске системе авиона и потпуно су интегрисане са системом за управљање летом и другим системима авионике.

као што су систем за забаву путника током лета (IFE систем) и системи управљања кабином (нпр. осветљење у кабини). Овај домен омогућава путницима да приступе интернету са својих личних уређаја (лаптопови и таблети).

Авиони су опремљени компјутерским мрежама и системима који размењују податке с пилотима, путницима, особљем за одржавање, другим авионима и контролорима ваздушног саобраћаја (сл. 7). Пораст повезаности мрежа и система авиона, као и других система путем интернета повећава простор за сајбер нападе. На пример, критични подаци, које користе системи у пилотској кабини могу бити измењени или подаци о лету могу бити намерно/злонамерно злоупотребљени од стране особе с овлашћеним приступом, затим, комерцијалне компоненте унутар система авионике могу садржати рањивости, које омогућавају сајбер нападе, а злонамерни хакери могу покушати да поремете операције лета различитим врстама напада на навигационе податке.

Уколико системи авионике нису адекватно заштићени, могу бити изложени ризику од потенцијалних сајбер напади. Као што је наведено у извештају GAO-21-86 [188], евидентирано је неколико кључних узрока **сајбер рањивости авиона**:

- **Рањивост софтвера** и дуги циклуси ажурирања комерцијалног софтвера – сложени комерцијални софтвери и компоненте, могу подржавати различите функције у авиону (нпр. уређаји за одржавање, као и уређаји посаде, који се конектују с њима). Уколико није потпуно изолован од спољашњих мрежа, такав софтвер неопходно је континуирано ажурирати у циљу заштите од новоидентификоване рањивости и променљивог сценарија претњи. Комерцијални софтвер има уграђене механизме за заштиту доступности и интегритета софтверског кôда, међутим, софтвер који се не ажурира правовремено, потенцијално је рањив на сајбер експлоатацију, услед спорог (некада и годину дана) и скупог (нпр. око милион долара, због неопходности бројних тестирања и евалуације, генерално) издавања модификација од стране програмера софтвера. Тако, дуги циклуси ажурирања остављају откривене рањивости, који могу имати импликације на сајбер безбедност авиона.
- **Ланци снабдевања** који нису на довољно високом безбедносном нивоу – ланац снабдевања је сложен, глобално дистрибуиран, међусобно повезан скуп ресурса и процеса који обухвата више различитих ентитета. У ваздухопловној индустрији, то је глобални систем добављача (нпр. произвођачи оригиналне опреме), пружаоца услуга одржавања, поправке и ремонта, као и клијента и авио-превозника – системи сваког од њих могу бити рањиви на различите сајбер претње. Без адекватне процене безбедносних пракси произвођача и студиозног тестирања електронских компоненти, рањивости сајбер безбедности могу се ″унети″ у системе авионике на више места/тачака унутар несигурних ланаца снабдевања У комерцијалним авионима, софтвер и хардвер компромитовани малвером могу омогућити злонамерним особама да изврше експлоатацију након инсталирања компромитованих компоненти. Затим, електронске хардверске компоненте авиона

(*line replaceable unit*)[79] могу бити угрожене и тако имати негативан утицај на лет. Такође је могуће да се ненамерно инсталирају фалсификоване *line replaceable unit* које садрже малвер или друге безбедносне претње.

- ***Upload* малициозног софтвера** – активности авио-компанија и аеродрома у вези с радом и одржавањем авиона, могу представљати рањивост инсталирањем злонамерног софтвера у системе авионике. На пример, злонамерни софтвер може се инсталирати на EFB (фуснота 78), тј. електронски уређај у власништву авио компаније, којим управљају пилоти и летачке посаде. Тренутно, EFB могу бити самостални уређаји (нпр. таблет) или интегрисани са системима као што је систем за управљање летом. Произвођачи развијају EFB-ове који могу преносити упутства, директно системима за управљање летом (током лета); уколико је такав EFB, повезан с авионом и заражен малвером, могао би омогућити DoS сајбер напад (део 2.1.2) или продор у друге конектоване *on-board* системе. У контексту аеродромских операција, рањивости на сајбер нападе представљају *gatelink* системи, тј. везе за пренос података/комуникације великог капацитета, које преносе податке између авиона и аеродрома. *Gatelink* системи су позиционирани на аеродрому близу гејта и конектују се с авиоником након слетања авиона. Уколико су ови системи заражени малвером, могли би утицати на кључне операције аеродрома. Нпр., након слетања авиона, *gatelink* системи се користе, између осталог, за аутоматски пренос података из авиона на путничке терминале, операције одржавања, руковање пртљагом и земаљску подршку. Компромитовани *gatelink* систем могао би да изазове сметње у раду ових аеродромских операција.
- **Застарели системи у авионима** старије производње– ризици по сајбер безбедност могу се повећати надоградњом или накнадним уграђивањем нових система електронике у авионе старије производње. Системи авионике у овим авионима, углавном нису повезани на интернет; при додатном опремању авиона новијим системима и побољшаном везом, важно је осигурати да софтвер и надоградње постојећих система буду без рањивости, што, како се истиче, представља веома велики изазов.
- **Лажирање података о лету** – авиони се ослањају на различите облике комуникације за извршење кључних функција, као што је слање и пријем података, који се односе на руте, навигацију и слетање. Ови комуникациони системи могу бити рањиви на нпр. лажирање (*spoofing*, део 2.1.2). На пример, одређени авиони су опремљени ADS–B системом, тј. ADS–B Out и ADS–B In (глава 6), који периодично емитује податке (нпр. идентификациони број лета, тренутна позиција, висина и брзина), који обезбеђује бољу комуникацију између авиона и ATC. Међутим, ова инфраструктура је незаштићена и отворена за сајбер нападе – комуникација између авиона и ATC је недовољно енкриптована и несигурна, тј. рањива на ометање и лажирање информација. У потенцијалном *spoofing* сценарију, измена информација о локацији авиона, онемогућава ADS–B земаљској станици да прими информације о правој локацији. *Spoofing* може утицати на свесност ситуације у авиону, стварањем авиона – "духова", што би могло довести до тога да пилот промени трајекторију лета авиона. Авиони користе комуникациону мрежу ACARS (део

[79] *Line replaceable unit* је модуларна компонента авиона, дизајнирана тако да се брзо замени током одржавања, у циљу минимизирања времена повратка система у оперативно стање.

3.1.2.2) за пренос порука/информација из авиона до корисника на земљи, тј. АТС-у (нпр. планове лета и информације о метеоролошким условима од АСТ), затим, за размену порука између система авиона и оних на земљи, као и за директно слање података системима за управљање летом. Како ACARS комуникације нису аутентификоване, могу бити пресретнуте, измењене или замењене лажним. Као што је поменуто, незаштићене ACARS комуникације могу бити лажиране/изманипулисане да би се послале лажне/погрешне поруке авиону (нетачне информације о позиционирању или лажни планови лета). Такође, истраживачи безбедности показали су да ILS (део 3.1.1) [189] који пилотима даје кључне податке о нпр. углу понирања и поравнању с пистом приликом слетања (нарочито ноћу и у условима магле), може бити нападнут заобилажењем физичке контроле приступа на земљи, као и пресретањем и лажирањем радио сигнала, које користи систем за слетање. Лажирање ових сигнала може довести до тога да инструмент за слетање покаже лажну путању лета авиона, што би могло проузроковати да пилот промени угао понирања авиона или брзину спуштања авиона, стварајући тако безбедносни ризик.

Карактеристике различитих комуникационих протокола ваздух–земља, као и врста потенцијалних сајбер напада на ове комуникационе технике (VHF говорна комуникација, CPDLC и ACARS), сумарно су дате у Табели 3.

За ублажавање сајбер рањивости, произвођачи авиона и авионике, постављају хардверску и софтверску заштиту, чиме се значајно смањује укупан ризик на безбедност авиона. На пример, уграђени умрежени системи на новим авионима подељени су у неколико независних домена. Сваки појединачни домен, садржи само системске функције, *data pathways* и податке неопходне за обављање функција успостављених за тај домен. Поред тога, домен контроле лета изолован је од свих других електронских преноса података из путничке кабине. Насупрот томе, дозвољена је, као и пожељна, једносмерна веза, која омогућава пренос неких података до путничке кабине (нпр. информација о статусу лета). Хардверске заштите укључују, између осталог, једносмерне електронске магистрале[80] за контролу правца тока података и уграђене аутоматске прекидаче за контролу активирања система (нпр. промене софтвера док је авион у лету). Софтверске заштите подразумевају тзв. заштитне зидове, који ограничавају саобраћај на мрежи и уграђене слојеве редунданције[81] у софтверу авионике, а који својим дизајном обезбеђују висок степен поузданости и спречавање кварова током лета. Поред тога,

[80] Електронска магистрала представља комуникациони систем за пренос података између рачунарских компоненти, више рачунара, или рачунара и улазно-излазних уређаја. Рачунарски систем садржи системску магистралу (повезује централну процесорку јединицу рачунара са главном меморијом, као и кеш меморијом другог нивоа) и одређени број улазно/излазних (I/O) магистрала (повезују различите периферне уређаје с централном процесорском јединицом, а која је повезана са системском магистралом преко "моста", инкорпорираног у процесорском скупу чипова); систем може имплементирати различите I/O магистрале, као што је PCI или USB магистрала.

[81] Редундантност се односи на било који систем у позадини, који се активира када постоји проблем, или увођење превентивних мера како би се проблем зауставио. То је широко заступљена технологија изградње рачунарских система, којом се постиже поузданост рада – рачунарски систем наставља да испуњава потребне задатке на задовољавајући начин и у присуству кварова, а који се јављају у хардверским и софтверским компонентама.

произвођачи подвргавају компоненте и системе авионске опреме, који су критични за лет, екстензивном тестирању, у циљу минимизирања могућих грешака у софтверу.

Табела 3. Карактеристике комуникационих протокола ваздух–земља (VHF говорна комуникација, CPDLC и ACARS) и врсте потенцијалних сајбер претњи на комуникационе протоколе (преузето и модификовано из [149]

Врста комуникационог протокола	VHF вербална (гласовна)	CPDLC	ACARS
Комуникација:	између земље и авиона	између земље и авиона	с авионом
Користи се за:	ATC инструкције или добијање других информација	ATC инструкције или добијање других информација	добијање података о позицији, времену, гориву, параметрима мотора, итд.
Сигнал:	Аналогни	дигитални	дигитални
Врста сигнала:	Емисиони	селективни	емисиони
Опсег фреквенција	117,975–137 MHz	VDL2*: 136,975 MHz CSC**	VDL2*: 136,975 MHz CSC**
Врста претње:	• Прислушкивање • Ометање (ненамерне радио сметње због нелиценцираних фреквенција • Ометање (неовлашћени приступ за блокирање VHF фреквенција • Лажирање (неовлашћени приступ за слање лажних инструкција између ATC и пилота)	• Прислушкивање (пресретање порука с подацима о саобраћају) • Ометање (блокирање канала) • *Flooding* (преношење кластера CPDLC података до примаоца) • Убризгавање (слање евентуално погрешних неовлашћених порука) • Алтернација (модификација садржаја поруке) • Маскирање (нападач се представља као овлашћени корисник, било да је авион-дух или ATC)	Промена плана лета, као и *weight/balance* у ACARS систему

*VDL2 – *VHF Data link – mode 2*
**CSC – *Common Signalling Channel*

Међутим, без обзира на предузете опсежне мере за спречавање сајбер напада, еволуирајући пејзаж сајбер претњи, у комбинацији са све већом употребом интерних мрежа у авионима и бројнијим везама између авиона и екстерних извора, потенцијално доводи до повећања ризика за безбедност летења у будућности. Тако, неколико истраживача сајбер безбедности истакло је ризике и показало рањивост *in-flight connectivity* система на годишњим *BlackHat* и другим професионалним конференцијама о сајбер безбедности. На пример, тим истраживача из Оксфорда, успео је да, користећи основну телевизијску опрему за кућну употребу и специјализован софтвер, прислушкује сателитске сигнале и тако приступи

подацима путника током лета. Поред тога, успели су да приступе подацима, које генерише таблет EFB-а повезан на мрежу авиона, а коју користи једна кинеска авиокомпанија [190].

Процес сертификације авио-компанија, укључује и тестирање сајбер безбедности. Након добијања сертификата, авио-компаније обавезне су да се придржавају програма безбедности авионске мреже, што подразумева адекватно одржавање интерне мреже авиона. Овај програм укључује и ″процес форензичке анализе за решавање инцидената у вези са сајбер-безбедношћу″, без спецификације за периодично тестирање у циљу смањења ризика. Међутим, у недостатку смерница FAA, тестирање ″трећих страна″, постаје све чешће, као нпр. у случају развоја најновијих сертификованих типова авиона (који су сада у употреби) авио-компанија *Boeing* и *Airbus*. Такође, *Boeing* је успоставио нови програм детектовања рањивости заснован на *web*-у, тако да независни истраживачи могу директно пријавити новооткривене потенцијалне претње. При свему овоме, неопходно је континуирано праћење *on-board* мрежа, затим, активности заснованих на етернету (фуснота 24), као и мрежа, које се заснивају на ARINC-429 стандарду [191].

Свакако, основа усвојеног приступа за повећање ефикасности авио-операција, је коришћење електронске размене података и дигиталне мрежне повезаности. При томе, IoT ће имати веома важну улогу [192]. Такође, побољшана оперативна ефикасност, смањење трошкова и рационализација управљања авио-саобраћајем, инкорпорирањем напредних ICT у авио систем, као што је поменуто, креира нови концепт, тј. *e-Enabled* авион (део 3.1.1). Ова визија интегрише многобројне различите врсте комуникационих технологија, као што су бежичне мреже сензора, ADS-B, LDCAS (*L-band Digital Aeronautical Communications Systems*)[82], сателити наредне генерације и мрежне технологије засноване на IP-у. Тренд повећања степена интеграције IT у механичке уређаје авиона, несумњиво ће повећати ефикасност, али и површину сајбер напада, као и његову пролиферацију [132]. Тако, коришћење техника вештачке интелигенције за аутоматизацију процеса напада од стране сајбер-нападача [194] изазива забринутост, али и стимулише стратегију одговора која се такође заснива на коришћењу оквира *Artificial Intelligence* (AI)[83] сајбер безбедносне одбране *e-Enabled* авиона.

---

[82] LDCAS је модеран телекомуникациони систем, заснован на најсавременијим техникама, које се користе у комерцијалним телекомуникацијама. Представља интегрисану CNS (*Communication, Navigation & Surveillance*) технологију. LDCAS намењен је за L фреквентни опсег (960–1164 MHz) и требало би да коегзистира с другим ваздухопловним системима из опсега, као што су DME и SSR транспондери [193].

[83] AI (вештачка интелигенција) је водећа технологија данашњице, тј. доба Четврте индустријске револуције (*Industry* 4.0 или 4IR), која се заснива на инкорпорирању људског понашања и интелигенције у машине/системе. Због тога је моделирање засновано на AI кључ за изградњу аутоматизованих, интелигентних и паметних система у складу с данашњим потребама. За решавање реалних проблема, могу се применити различите врсте AI као што су аналитичка, функционална, интерактивна, текстуална и визуелна. Међутим, развој ефикасног AI модела је изазован задатак због динамичке природе и варијација у проблемима и подацима из реалног света. Свакако, развијене AI технике могу играти важну улогу у развоју интелигентних и паметних система у различитим областима, као што су сајбер безбедност, пословање, финансије, здравствена заштита, пољопривреда, итд. [195].

3.1.2.3. Авио компаније

Авио компаније користе савремене IT у циљу повећања ефикасности пружања услуга (пораст функционалности *web*-а, као што је побољшање *online* канала за куповину/креирање/промену/отказивање резервације путовања, повећање самосталних операција путника, као што је увођење система за управљање изненадним променама летова, система за информације о изгубљеном пртљагу, самостално "чекирање", итд.), смањењу трошкова, као и повећање прихода авио компаније (проширење сервиса, подршка динамичког креирања путовања, итд.). Тако, авио компаније инвестирају у савремене IT, и то пре свега, у операције, које се односе на путнике, авионе, летове, али и безбедност.

Као што је поменуто, сајбер безбедносне претње на авио компаније, укључују ризике од *web* апликација, као што је *Sykipot backdoor tool*, као и експлотације *Twitter* налога, које могу угрозити рад и репутацију авиокомпанија. Поред тога. нападима могу бити изложени и сајтови аеродромских управа, од стране политички мотивисаних нападача. За сајбер нападе на мреже и веб-сајтове, користе се различити алати. Поменути *Sykipot* инфицира мету *spear-phishing* техником (*e-mail* или електронска комуникациона превара), слањем *e-mail*-ова с малициозним прилозима у циљу инсталирања *malware*-а на рачунар корисника или крађе/прикупљања података о цивилном авио сектору USA, с још увек непознатим намерама [4]. Тако, *Sykipot* кампања (2013), имала је циљане сајбер нападе на потенцијалне учеснике 2013 IEEE *Aerospace Conference*, тј. ваздухопловне стручњаке, академике, припаднике војске и руководиоце различитих авио сектора, слањем лажних е-мејлова. За малициозне хакере, мете су оперативни систем или апликације, као што су *Web browsers* и *Java*. Малициозни хакери користе и DDoS нападе (део 2.1.2). Тако, израелска национална авио компанија El-Al била је главна мета политички оријентисаног сајбер напада (2012), које је предузела хакерска група "*Nightmare Group*", док је према тврдњама (2013) хакерске група "*Qods Freedom*", хакована и уклоњена *web* локација El-Al-а, као и других циљаних израелских *web* локација у планираном DDoS нападу 2013. године [4].

Обезбеђивање квалитетнијих конекција, коришћењем *on-board* Wi-Fi везе или развојем *e-Enabled* авиона, излаже авио компаније значајним безбедносним ризицима широког спектра. Због тога, ове везе морају бити одвојене од *on-board* веза, тј. веза које се користе за авионске операције.

3.1.2.4. Аеродроми и пограничне власти

Експоненцијални пораст броја путника, захтева еволуцију тренутних логистичких и инфраструктурних концепата аеродрома, како би се брзо и одрживо прилагодили. Међутим, нови изазови с којима се авио сектор мора суочити и коме се мора прилагодити, је нпр. интеграција IoT (део 2.1.1.2) у аеродромске објекте, као и све већа употреба паметних уређаја од стране путника и запослених. Сајбер безбедност постаје кључни фактор безбедности, а аеродроми, у настојању да обезбеде оптималне услуге на поуздан и одржив начин, константно раде на унапређењу ефикасности, безбедности и сигурности.

Први важан корак у разматрању сајбер безбедности аеродрома, је разумевање врсте и извора претњи, тј. радњи које могу негативно утицати на рад или имовину аеродрома, с којима се суочавају. Разумевање претњи на рањивости аеродромских система, важно је због предузимања контрамера, а у складу са постојећим ресурсима (аеродроми, агенције, организације и стручњаци за сајбер безбедност, који се баве одређеним аспектима сајбер претњи, актерима и мотивима напада).

Аеродроми комерцијалне авијације састоје се из одређених области, које имају различите безбедносне нивое, тзв. **безбедносне области**, и то (сл. 8):

- *Air operations area (*AOA) – део аеродрома где се спроводе безбедносне мере и обухвата: маневарске површине (део за таксирање авиона), области за паркирање авиона, рампе за утовар/истовар и области за генералну авијацију.
- *Secure area* – област у којој се врши укрцавање/искрцавање путника, као и утовар/истовар пртљага.
- *Sterile area* – део аеродромског терминала у коме се могу налазити искључиво путници, који су прошли *passenger screening checkpoints* или *security*; данас, овој области имају приступ само путници, који имају авионске карте.
- *Security identification display area* (SIDA) – укључује безбедне зоне и друге могуће зоне аеродрома; приступ овој области имају само особе са идентификационим картицама, или особе у пратњи овлашћене особе.
- *Exclusive area* – обухвата хангаре, *air cargo* просторије, као и *hendling* оператере, тј. *fixed-base operators*, FBOs, који опслужују генералну авијацију и чартере).

Слика 8. Безбедносне области аеродрома (USA) (слика модификована и преузета из [197])
TSA – *Transportation Security Administration*; SIDA – *Security identification display area*; AOA – *Air operations area*

Остале области аеродрома подразумевају јавне површине и не подлежу директно безбедносним прописима, који се односе на ограничени приступ. SIDA и AOA најчешће обухватају области за утовар пртљага, као и области у непосредној околини терминала, паркираних авиона и аеродромских објеката. Неки аеродромски оператери могу све AOA области дефинисати као SIDA области [196].

Аеродроми су сложена окружења с јединственим изазовима који, за ефикасно функционисање, захтевају IT менаџмент са специфичним знањем, широким могућностима и разноврсним услугама. С развојем нових система и технологија, које су доступне не само менаџменту и особљу аеродрома, већ и авио компанијама, као и путницима, број и ширина сајбер система аеродрома се повећава. Тако, неки аеродроми се умногоме ослањају на јавне мобилне или бежичне мреже како би проширили домет својих сајбер система на терминалима и аеродромима. Такође, неки аеродроми омогућавају својим запосленима коришћење BYOD уређаја (фуснота 44), тј. личних телефона и таблета за обављање својих радних обавеза. Дакле, ширина система аеродрома није ограничена само аеродромском мрежом или објектима – све већи број аеродрома ослања се на рачунарску инфраструктуру, софтвер, као и податке, који су на интернету или у ″облаку″. Тако, напредак у интеграцији IoT уређаја унутар инфраструктуре сектора ваздухопловства, довео је до појаве ″паметног″ аеродрома[84] [199]. У суштини, **паметни аеродром** (фуснота 49) је систем богат подацима и садржи бројне сензоре, актуаторе и друге уграђене уређаје, који корисницима омогућавају кориснички интерфејс за интеракцију са сајбер-физичким уређајима у окружењу (сл. 9). Тако, аеродроми имплементирају технолошке иновације, због чега побољшавају своју ″инфраструктурну интелигенцију″ и развијају се као паметни објекти који подржавају пораст броја путника и обезбеђују пријатно искуство путовања.

С порастом броја и ширине сајбер система који се користе на аеродромима, повећава се и осетљивост аеродрома на **унутрашње и спољашње сајбер претње**, као и нападе криминалаца, терориста[85] или проблематичних путника.

[84] Развој IoT, довешће до трансформације најпрометнијих аеродрома у модерне, паметне аеродроме. Од паметних апликација на аеродромима [198], највише се користе услуге пријаве и укрцавања путника (41%) и системи за процесирање путника широке употребе (41%), затим, везе са другим транспортним системима, а најмање SCADA апликације (6%), које су у почетној фази имплементације. Међутим, на паметним аеродромима, веома су заступљене IoT апликације (>70%), као што су руковање пртљагом, пријављивање путника, контроле операција у оквиру *landside* зоне, системи за процесирање путника широке употребе и веб услуге за путнике, затим, системи управљања зградом и контроле опреме за грејање, вентилацију и климатизацију (60%), као и SCADA (20%).

[85] Терориста је особа, која употребљава насиље/претње у циљу застрашивања/присиле, најчешће за остваривање неког политичког циља. Терористички акт није импулсивна радња, већ је резултат детаљног планирања, у којима се процењују слабе тачке, тј. рањивости мете. Ово имплицира веома комплексну превенцију тероризма, као и примену принципа ″слојевите″ безбедности за његово спречавање. Постојање неколико слојева (појасева) безбедности омогућава да, иако један од појасева буде пробијен, целовитост безбедносног система ипак остаје очувана. Најтежи облик и највећи безбедносни изазов , јесте самоубилачки терористички акт (једноставан и јефтин напад), у коме терориста бира време, место и околности напада, што ствара осећај велике беспомоћности и страха у друштву, као и значајно отежава предузимање превентивних мера.

Криминалац[86], у контексту безбедности аеродрома, јесте особа, која предузима радње, које имплицирају ризике од повреда, опасности, губитке живота/имовине. Проблематични путник је особа која показује неприродно, ненормално или увредљиво понашање на аеродрому/комерцијалном лету. Ова особа нема *apriori* намеру изазивања штете, а њено проблематично понашање узроковано је неким догађајем, који је на особу деловало узнемирујуће (гужва, лична фрустрација и сл.), коришћењем недозвољених супстанци (нпр. алкохола, пре и током лета, и сл.), итд.

Слика 9. Комуникациони интерфејси "ствари" (модификовано и преузето из [200])

Осим класичне ICT инфраструктуре (интернет и е-пошта), потенцијалне **мете сајбер напада** из домена **унутрашњих аеродромских операција**, могу бити: контрола уласка и системи за детекцију покушаја "пробоја" периметра (*perimeter intrusion systems*), авионски системи (у функцији), радарски системи, земаљски радар, *network-enabled* систем[87] пртљага, мрежни системи (бежични и жичани), управљање објектом, јавне службе, контрола надзора и прикупљање података (SCADA)-тип ICS (*Industrial Control Systems*), итд. [152, 201].

С обзиром на све већу употребу мобилних апликација, као и хардвера, примарну бригу представљају **сајбер претње** на аеродромске **интерне операције**. На пример, *Heathro*-ов (Лондон) терминал 5, је огромна IT инфраструктура, чију функционалност подржава 1.500 камера CCTV система (интерни систем камера),

[86] На пример, криминалци чији је циљ крађа терета, могу то учинити насилно, док је авион на земљи, или могу, након укрцавања, отети авион и приморати пилота да слети на одређену локацију. У оба случаја, криминалци унапред познају карактеристике терета, лета као и начине да заобиђу безбедносне провере. У томе им могу помагати особе, тзв., корумпирани инсајдери, који такође спадају у ову групу починилаца штете (групу криминалаца).

[87] *Network-enabled* систем јесте систем који може да се повеже на интернет или се користи на интернету.

1.100 безбедних приступних контролних тачака, *Wireless Local Area Network* (WLAN)[88] са 750 приступних тачака и 2.800 телефона базираних на хибридној архитектури аналогне, дигиталне и IP телефоније, а који су рањиви на сајбер претње[89] [137].

Аеродромске **рачунарске мреже рањиве** су на сајбер нападе преко [137]: USB драјвова, USB уређаја (дигиталне камере, MP3 плејери, итд.), лаптопова и нотбукова, бежичних приступних тачака, апарата и уређаја које запослени позајмљују другима, *Trojan Human* (нападачи који посећују сајтове лажно се представљајући као запослени), оптичких медиа (CD, DVD, итд.), недостатка пажње запослених, ″паметних″ телефона, е-мајлова, социјалних мрежа, циљаних *botnet* напада, DDoS напада (део 3.1.1), ексфилтрације података[90] и инсајдер претњи, онлајн превара, итд. Као што је поменуто, на радним местима је уобичајено коришћење **BYOD** уређаја (*iPhones, iPads, Anroid* и *Tablets*), а на аеродромима, осим корисника аеродромских услуга, употребљавају их и запослени. Ови уређају комуницирају с екстерним системима (*e-mail* или VPN приступ), тако да могу бити извор рачунарских вируса (део 3.1.1), или се потенцијално користити за прикупљање поверљивих информација. Многи аеродроми подржавају политику коришћења BYOD уређаја, тј. запосленима на аеродрому је омогућено да, преко личних налога (шифри) конектују своје неодобрене/нерегистроване личне уређаје на безбедне мреже, а како се показало, тако излажући мрежу безбедносним ризицима [137]. Неке од технологија, које се користе за отклањање опасности од конектовања BYOD уређаја на корпорацијске мреже су нпр. *Wireless Intrusion Prevention System* (WIPS), *Network Access Control* (NAC) и *Mobile Device Management* (MDM). Слично, озбиљне сајбер претње проузроковане су и повећањем броја **Wi-Fi хотспотова**[91], с обзиром на то да се хардверски захтеви за мобилне хотспотове смањују, јер се могу креирати и *smart* мобилним уређајима запослених. Процена је да око 20% компанија, у неком тренутку, има у својим

[88] WLAN је бежична LAN (*Local Area Network*) мрежа, која омогућава бежично повезивање и бежичну међусобну комуникацију уређаја. За разлику од жичаног LAN (комуникација између уређаја остварује се екстерним кабловима), код WLAN, комуникација између уређаја остварује се преко Wi-Fi везе. Тренутно, већина рутера су бежични и представљају базне станице, које омогућавају бежичне везе са сваким Wi-Fi повезаним уређајем (лаптоп, паметни телефон и сл.), а који је у опсегу бежичног сигнала рутера. Бежични рутери су често конектовани с кабловским модемом или другим уређајем, који је повезан на интернет. Тако, LAN и WLAN се могу повезати, а бежични рутери, најчешће, спајају *externet* и Wi-Fi повезане уређаје у исту мрежу, што омогућава да жичани и бежични уређаји међусобно комуницирају путем једног рутера.

[89] Осим великих аеродрома, и свакодневно пословање малих аеродрома, у значајном обиму зависи од рачунарских умрежених система, тако да и они могу бити потенцијалне мете различитих сајбер напада [202].

[90] Ексфилтрација података је неовлашћено копирање, пренос или проналажење података са рачунара/сервера, тј. извоз/крађа података.

[91] *Hotspot* (приступна тачка) јесте физичка локација (место) на којој се може приступити интернету, најчешће користећи Wi-Fi технологију преко бежичне и локалне мреже, користећи рутер (повезан са интернет провајдером).

мрежама *Rogue Access Points* (APs)[92], а што утиче на то да мрежа постане отворена за бројне сајбер нападе. Запослени могу несвесно унети вирус и омогућити приступ малициозним корисницима, посећивањем реномираних сајтова или социјалних мрежа, слањем е-мејлова или преко USB драјвова. На пример, анализа безбедности безичне мреже (*Gartner Mobile and AirTight Networks*) спроведена на 14 аеродрома у USA, Канаде и Азије [203], показала је да ови аеродроми користе отворене и слабо обезбеђене *wireless* мреже – од Wi-Fi детектованих мрежа, 77% су приватне (*non-hotspot*) небезбедне мреже, које користе застарели и веома лош WEP (*Wired Equivalent Privacy*) систем шифровања; неке од ових Wi-Fi мрежа различитих система (систем за издавање карата, систем за пртљаг, као и систем аеродромских продавница и ресторана), користе се, такође, за критичне аеродромске операције и логистику. Поред тога, истраживање је показало да само 3% корисника мобилних уређаја употребљава VPN, док је 10% лаптопова било инфицирано вирусом преко Wi-Fi мреже.

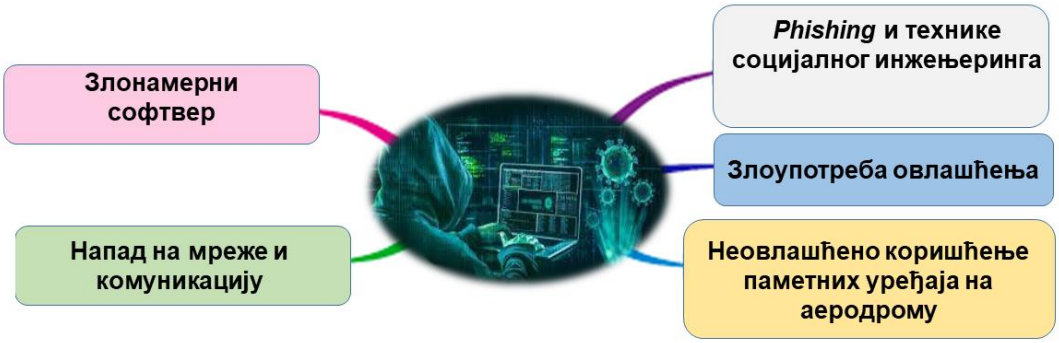
Тако**, сајбер претње** на **паметне аеродроме**, тј. напади на IoT инфраструктуре и апликације у оквиру паметних аеродома, могу се генерално поделити на [198]: нападе на комуникационе мреже, злонамерни софтвер, манипулисање IoT уређајима аеродрома, *phishing* (део 3.1.1) и технике социјалног инжењеринга, злоупотреба овлашћења и неовлашћено коришћење паметних уређаја на аеродрому (сл. 10). IoT системи и уређаји су подложни *Advance Persistent Threat* (APT)[93] нападима, због хардверских ограничења, грешака у софтверу или погрешних конфигурација [199]

Сајбер безбедност аеродрома, дефинише се као превенција и/или реакција на смишљене злонамерне активности предузете коришћењем електронике/рачунара на аеродромске системе – мете, директно, или индиректно, онде где ови системи имају кључну улогу у ширем ваздухопловном систему. Робустан оквир сајбер-одбране на паметним аеродромима је од виталног значаја да би се осигурала поузданост услуга и ублажила опасност од прекида и отказивања услуга, као и губитка осетљивих информација. Најновије, за развој безбедносних решења за

[92] *Rogue Access Point* јесте приступна тачка инсталирана на безбедној мрежи без изричитог овлашћења локалног администратора мреже, како од стране добронамерног службеника, тако и од злонамерног хакера.

[93] APT је продужени и циљани сајбер напад у коме актери/хакери добијају приступ мрежи и остају неоткривени током дужег временског периода. Циљ већине APT је крађа података, а није наношења штете мрежи мете (национална држава и велике корпорације). За приступ мрежи, APT често користе напредне методе напада, укључујући напредне експлоатације рањивости нултог дана, као и *spear phishing* и друге технике социјалног инжењеринга. Мотиви APT су различити, као нпр. нападачи које спонзоришу националне државе могу циљати интелектуалну својину у циљу стицања конкурентске предности или финансијске добити. Ексфилтрација података мете, указује на APT, а стручњаци за сајбер безбедност често се фокусирају на откривање аномалија у излазним подацима како би утврдили да ли је мрежа била мета APT напада. Неке од APT група су APT28 (руска APT, позната као *Fancy Bear*, *Pawn Storm*, *Sofacy Group* и *Sednit*, која се доводи у везу с нападима на војне и владине циљеве у источној Европи, укључујући Украјину и Грузије, као и кампање усмерене на NATO), APT29 (руска APT, позната као *Cozy Bear*), иранска APT34 (циљеви су биле финансијске, владине, енергетске, хемијске и телекомуникационе компаније Блиског истока) и Северно Корејска APT37 (позната као *Reaper*, *StarCruft* и *Group* 123) [204].

нападе инспирисане IoT-ом, предлажу се AI технике засноване на машинском учењу(фуснота 83) [205].



Слика 10. Врсте злонамерних претњи на сајбер безбедност паметног аеродрома

Дакле, иако на први поглед није уочљиво, ICT аеродрома рањиве су на сајбер напад, без обзира на то да ли су, или не, конектовани на интернет. Као што је поменуто, Wi-Fi мреже, које се користе за јавни приступ интернету или безбедне аеродромске операције, такође уводе јединствене рањивости. Штавише, аеродроми се све више ослањају на бројне IT услуге које су у "облаку", односно базиране су на подацима "треће стране", којима се приступа путем интернета. Такође, аеродроми, FAA и авио-компаније све се више ослањају на GPS у циљу обезбеђивања оперативне сигурности и ефикасности. У контексту аеродрома, менаџери и особље аеродрома, али и екстерни пружаоци услуга, који инсталирају, конфигуришу, руководе и одржавају аеродромске системе, морају преиспитивати **сајбер против-мере**, а које су специфичне за њихове системе.

Тако, примарне активности за унапређење сајбер безбедности подразумевају [206]:

- константно спровођење идентификације опреме, софтвера, пословне праксе и дистрибуције података унутар организације, њене мреже и подмреже
- заштититу система, података и инфраструктуре, спровођењем и ажурирањем против-мера
- благовремено детектовање сајбер напада праћењем аномалних активности на крајњој тачки система, IT и комуникационим мрежама, као и областима с осетљивом IT и ITC инфраструктуром
- брз и ефикасан одговор на сајбер напад, тако минимизирајући његово трајање и утицај (ефикасан одговор почиње пре него што до напада дође, планирањем реакција и прикупљањем информација/контаката који могу бити од помоћи).

Дакле, због све већа употребе ITC на аеродромима, у циљу подршке корисничким сервисима [207], побољшању операција авиона и безбедности [208], као и остваривању одрживости [209] и других стратешких циљева, аеродроми постају изложенији претњама по њихове дигиталне податке и електронске системе. Број и софистицираност ових сајбер претњи се повећава [210], као и број појединаца

и организација (тзв. актера) који изводе сајбер нападе. Државе, организоване криминалне групе и корпорације улажу значајна средства у ове нападе, а с порастом пролиферације међусобно повезаних електронских уређаја и њихове употребе, овај тренд ће се вероватно и наставити.

Свакако, тврдња – „ако није повезан на интернет, није подложан сајбер нападима.", нажалост, није тачна, што су доказали многи успешни напади који нису изведени коришћењем интернета [206]. Иако су бројне сајбер претње спречене, исте константно расту, као и забринутост у вези са сајбер ризицима, и то нарочито ако се узму у обзир успешно реализовани сајбер напади на аеродроме (систематизовано у делу 7).

4. УПРАВЉАЊЕ САЈБЕР БЕЗБЕДНОСНИМ РИЗИЦИМА

> *"У свету сталних и динамичних технолошких промена, минимизирање рањивости је бесконачна трка са противницима. Будућем развоју ваздухопловне индустрије и применама нових технологија, прилагођаваће се и сајбер претње. Због тога, неопходна је континуирана ревизија постављених стратегија, усклађених с променама у вези са сајбер претњама, технологији и регулативама, истовремено подстичући регулаторно окружење да прихвати иновације."* [211]

Термин сајбер безбедност је често субјективан, а свеобухватно дефинисање појма (поглавље 2.2.) наставља да се развија с напретком модерне технологије. Сајбер безбедност, често се доводи у везу са сложеном технологијом и злонамерним манифестацијама кршења безбедности, при чему се, неретко занемарују људски и процесни аспекти остваривања безбедности, као и могућност случајног нарушавања безбедности или безбедносног надзора.

Концепт сајбер криминала, односно сајбер напада и сајбер тероризма [212] је застрашујући (део 2.1.1.2), с обзиром на свеприсутност ICT (од личног простора појединца, преко радног места, до јавног простора, и с њима је у константној интеракцији) и огромних могућности, тј. предности које имају сајбер криминалци у злонамерној активности, а што се односи на анонимност и незнатна финансијска улагања[94]. Ваздухопловство је прво на листи индустрија које интегришу нове ICT, у циљу побољшања кључних авио процеса (системи за руковање пртљагом, системи за приказивање информација о лету и сл.), а усвајање иницијативе за нови сервис – самопослуживање путника у авиону[95], надоградњу ATM технологија и бежичних система за забаву путника током лета, само су неки од примера који потврђују све већи "улазак" авио сектора у сајбер простор. Иако постоје бројни бенефити, овај развој авио система повећава сајбер рањивости на ICT авио системе, због чега је неопходно посветити нарочиту пажњу идентификацији сајбер ризика и увести одговарајућа ублажавања истих.

Сајбер ризик представља ризик од финансијског губитка, поремећаја у раду или штете, због квара дигиталних технологија које се користе за информационе и/или оперативне функције уведене у производни систем путем електронских средстава од неовлашћеног приступа, употребе, откривања, прекида, модификације или деструкције производног система [215]. Да би се у потпуности применила пракса управљања ризиком, морају се узети у обзир сви кључни фактори ризика. При томе,

---

[94] Тако, најбрже растући сајбер криминал јесте *ransomware* (део 3.1.1), који не захтева значајна финансијска улагања за инсталирање (око 200 $), а има огромни штетни ефекат на појединце/корпорације [213].

[95] На пример, *Lufthansa* је прва компанија која је увела нови сервис за путнике (2017) у авиону *Airbus* A350-900 – у специјално дизајнираном делу за самопослуживање, путници (бизнис класе) могу се сами послужити освежењем између оброка. Такође, овај тип авиона, захваљујући специјалном концепту осветљења, ергономски дизајнираним седиштима и повећаном простору за личне ствари, омогућава веома удобно путовање [214].

у процени заштите сајбер безбедности, приступ који се заснива на претњама[96], омогућава адекватну заштиту од реалних претњи по сајбер безбедност, утврђивањем величине покривености постојеће заштите, идентификацијом недостатака (места/области без адекватне заштите, тј. области где постоје претње) и преклапања (области у којима вишеструке заштите од истих врста претњи, непотребно повећавају трошкове).

Главни елементи сајбер безбедности и њеног управљања су различите сајбер претње: сајбер криминал[97], сајбер ратовање[98], сајбер тероризам[99] (описани у делу 3), сајбер шпијунажа[100] и хактивизам[101] [90], и изазови у њиховом управљању.

Узимајући у обзир да је ваздухопловни систем, један од критичних инфраструктурних сектора и важан ресурс сваке државе, њена је обавеза, као и одговорност, да константно јача и унапређење ниво сајбер безбедности сектора цивилне авијације. За **остваривање сајбер безбедности**, неопходно је:

- међусобно повезивање и јачање сарадње између свих сектора друштва (цивилних, полицијских, војних, привредних и академских институција),

---

[96] Допуна претњама је концепт рањивости – оба су неопходна да би се десио догађај/сценарио (мора постојати претња, да би се искористила рањивост); рањивост је слабост у информационом систему, безбедносним процедурама система, интерним контролама или имплементацији, које се могле искористити извором претњи.

[97] Сајбер криминал је релативно нови, веома опасан облик криминалног понашања, тј. криминалне делатности, која се предузима употребом рачунара/рачунарских система и мрежа; обухвата различита кривична дела извршена у сајбер простору, као што су дела против поверљивости, интегритета и доступности компјутерских података и система, дела у вези са рачунарима (фалсификовање и крађе), затим, са садржајима (нпр. дечија порнографија), као и са кршењем ауторских и сродних права.

[98] Сајбер ратовање (део 2.1.1.2**)** је врста политичке претње, у случају када је напад предузео неки субјект међународног права у циљу акта агресије над другим субјектом међународног права [91].

[99] Сајбер тероризам подразумева нападе на рачунарске системе/мреже, који могу бити физички (употреба конвенционалног наоружања у циљу уништења или озбиљног оштећења ICT ресурса), електронски (употреба електромагнетског зрачења високе енергије) и напади на рачунарске мреже и системе (употреба малициозног кода), сви у циљу остваривања политичких циљева [91].

[100] Сајбер шпијунажа представља радњу која се предузима у тајности/под лажном претпоставком, користећи сајбер капацитете за прикупљање/покушај прикупљања информација у циљу њиховог преношења супротној страни. Једна од основних карактеристика сајбер шпијунаже јесте изражена асиметрија трошкова – новчана улагања нападача, који треба да открије и искористи само једну слабу тачку, неупоредиво су мања од улагања у заштиту и одбрану од свих слабости. Затим, процена је да је за откривање упада у систем, потребно од један до три месеца, током којих нападач може имати на располагању широк спектар информација. Такође, сајбер шпијунажа омогућава добијање већег обима осетљивих информација о противнику, с обзиром на глобалну присутност интернета и мрежних услуга.

[101] Иако у погледу последица, хактивизам изазива мању штету (користи тактике ширења црва и вируса, DDoS нападе, итд.), веома је танка граница између хактивизма и сајбер напада (видети Табелу 1) – у неким случајевима, хактивисти могу сарађивати са сајбер криминалцима, затим, спроводити активности преузимања корисничких налога *Tweeter*-а и *Facebook*-а, као и незаконито преузимати и/или откривати поверљиве информације, а директне претње неких хактивиста владама/корпорацијама/појединцима могу потенцијално изазвати панику/страх код цивилног становништва.

уз узајамно поверење и размену информација о безбедносним рањивостима, што је основни услов за успешну сарадњу јавног и приватног сектора[102]

- постојање индивидуалне одговорности, као и одговорности пословног сектора
- међуинституционална сарадња (суштинска у ефективној и ефикасној сајбер безбедности и обезбеђивању партиципативне и одговорне сајбер политике
- међународна сарадња у процесу доношења сајбер стандарда[103] и безбедносних мера заштите ICT мреже од познатих сајбер претњи, како би се најефикасније искористиле предности, способности и искуства заинтересованих, као и примена безбедносних стандарда и механизама у сопственој безбедносној легислативи; значајан пример је сарадња авио компаније *Boeing* и Националног института за стандарде и технологију USA, који је овој компанији доставио опсежне податке о тренутним праксама управљања ризицима, најбољим решењима и стандардима, као и специфичним праксама, које се користе у индустрији, а које су релевантне за авио сектор
- доношење адекватних мера, одговарајућих законских оквира и политика, које морају поштовати слободан приступ информацијама и друге демократске принципе.

У циљу разумевања сајбер ризика/рањивости и потенцијалних последица, које ови ризици могу имати на функционисање авио система, управљање сајбер ризицима и предузимање одговарајућих мера заштите, затим, ефикасно реаговање и опоравак од сајбер инцидента, промовисање културе безбедности мрежа и података, као и повећање свести о сајбер безбедности и изградњи адекватне сајбер архитектуре, неопходно је постојање **сајбер безбедносних стратегија** (поглавље 4.1). При томе, и јавни и приватни субјекти у авио сектору, требало би да узму у разматрање сајбер безбедносне стратегије у другим индустријским секторима. С друге стране, кроз сарадњу сајбер безбедносних регулатора и водећих субјеката у авио индустрији, требало би константно промовисати добру сајбер безбедносну праксу у широј ваздухопловној заједници; то укључује енкрипцију и трансфер личних података и безбедносну заштиту за COTS (фуснота 52), као и неподржавање/суспензију лоше праксе, која је узрок рањивости сифтвера, хардвера и авио система. Такође, у заштити авио система од сајбер ризика/рањивости, неопходно је континуирано унапређење постојећих сајбер безбедносих стратегија[104].

---

[102] На пример, јавни и приватни сектор, све фреквентније, размењују информације у циљу превенције и детекције сајбер инцидената; у односу на јавни сектор, приватне компаније често располажу напреднијим технологијама и знањима, које могу учинити транспарентним, у циљу повећања целокупне сајбер безбедности у држави, тако повећавајући безбедност и свог пословања.

[103] Како је ваздухопловни систем, један од критичних инфраструктурних сектора и важан ресурс сваке државе, авио индустрија, у односу на друге гране транспортног саобраћаја, јесте водећа и најнапреднија грана у погледу коришћења сајбер безбедносних стандарда.

[104] На пример, авио-компанија *Boeing* у сарадњи с авио индустријом развија јединствени *Cyber Technical Center* за процену угрожености од сајбер претњи и дизајнирање сајбер заштите својих авиона, што ће обезбедити неопходну сајбер безбедност за кориснике.

Након дефинисања циљева сајбер безбедности, неопходно је одредити улоге и одговорности различитих субјеката у постизању циљева (поставити адекватан оквир управљања), и јасно их дефинисати међународним законима и стандардима (правни оквир) авио сајбер безбедности (део 4.1.1).

Сајбер безбедност у **цивилној авијацији**, остварује се сарадњом националних агенција, приватних субјеката и међународних организација (део 4.1.2). Као што је поменуто, за сајбер безбедност у ваздухопловству, неопходне су нове стратегије, које наглашавају сарадњу свих зауинтересованих субјеката и међусобну размену информација, као и јасну атрибуцију одговорности. Слично приступима који се користе нпр. у сектору јавног здравља, регулаторни органи за сајбер безбедност у сектору цивилне авијације, авио индустрија и међународне организације, као што су ICAO и IATA, могу сарађивати и заједно радити на утврђивању одговорности различитих заинтересованих субјеката.

Сајбер напади могу се спречити слично начину који користе сајбер преступници за њихово извођење, а то је блокирањем сигнала, или хаковањем за преузимање контроле. Адекватан одговор на сајбер напад, подразумева и адекватну сајбер безбедносну обуку, као и положен одговарајући сертификациони испит за оператере. Такође, од изузетног значаја је процена целокупног спектра претњи (не само најопаснијих претњи), тј. развијање методологије процене сајбер безбедности (поглавље 4.2) у циљу адекватног разумевања ризика, које имају по људе, институције и економију, као и управљање тим ризицима.

4.1. САЈБЕР БЕЗБЕДНОСНЕ СТРАТЕГИЈЕ

Сајбер напади на авио систем остварују се подсредством различитих система, платформи и технологија, које унапређују сигурност и ефикасност путовања. Иако се сматра да је ризик од успешног терористичког сајбер напада с губитком људских живота, у односу на друге облике тероризма, релативно низак [5], чињеница је да **сајбер претње** могу имати значајан утицај и озбиљне штетне последице на безбедност, оперативни и финансијски интегритет, као и репутацију авио сектора у целини, а с обзиром на број, динамику и непредвидивост ових претњи. Такође, не би требало ни занемарити озбиљне ризике и претње у вези са шпијунажом (фуснота 100), тј. прикупљању информација у вези са инфраструктуром и запосленима, што може допринети планирању физичких или будућих сајбер напада на авио сектор.

Јасно је да су сајбер напади/инциденти на авио систем реалност (део 7). Међузависност и међуповезаност авио операција и ICT, захтева и развијање тзв. хибридног система, који спаја елементе авио- и индустрије ICT, обезбеђујући адекватно окружење за безбедно и сигурно функционисање. То подразумева и осмишљавање специфичне "архитектуре сајбер безбедности". Први корак у том правцу, јесте сагледавање комплетне слике, тј. разумевање, идентификовање и прихватање постојања сајбер претњи, као и схватање импликација повећања повезаности и зависности авио система од ITC, у светлу развоја сајбер ризика/претњи. У вези са правном регулативом, а с обзиром на јединствену природу сајбер простора и различите активности, чак и ако нису донети посебни закони за борбу против сајбер напада, неопходно је, у локалне кривичне законе,

имплементирати одговарајуће одредбе и регулативе (део 4.2). Посебна архитектура сајбер безбедности авио система, може се градити успостављањем заједничких стандарда, чиме се задржава јака и и затворена структура, која обезбеђује строгу регулацију и контролу. Поред тога, неопходно је успостављање сајбер-безбедносне културе, кроз формулисање и имплементацију *Standards and Recomended Practices* (SARP). За ефикасно спровођење културе сајбер безбедности, потребно је континуирано подстицање координације и сарадње између држава, као и субјеката из индустрије, као и транспарентности и дељењу информација, тј. успостављање система за извештавање о сајбер-безбедносним инцидентима. Такође, компоненте за пренос података, и то нарочито COTS уређаји, морају имати одговарајућу заштиту од сајбер напада, а произвођачи имати обавезу да обезбеде минималне сајбер-безбедносне стандарде.

Који су кораци које предузима авио индустрија у сарадњи са ICAO и националним законодавством у циљу решавања проблема у вези са растућим таласом сајбер криминала? У погледу глобалних захтева, ICAO *Annex* 17, за безбедност у ваздухопловству, укључујући и сајбер безбедност, поставља стандарде високог нивоа за безбедност у ваздухопловству, којима ће ″свака држава успоставити и применити писани национални програм безбедности цивилног ваздухопловства″ и, у погледу *Air Navigation Service Providers* (ANSPs)[105], ″пружаоце услуга ваздушног саобраћаја који раде у тој држави да успостави и примени одговарајуће безбедносне одредбе како би испунили захтеве програма националне безбедности цивилног ваздухопловства″. За усклађивање са стандардима ICAO, постављен је оквир за сајбер безбедност националне инфраструктуре, базиран на тренутно најбољим праксама у области сајбер безбедности, као што је сумирано на сл. 11 [216].

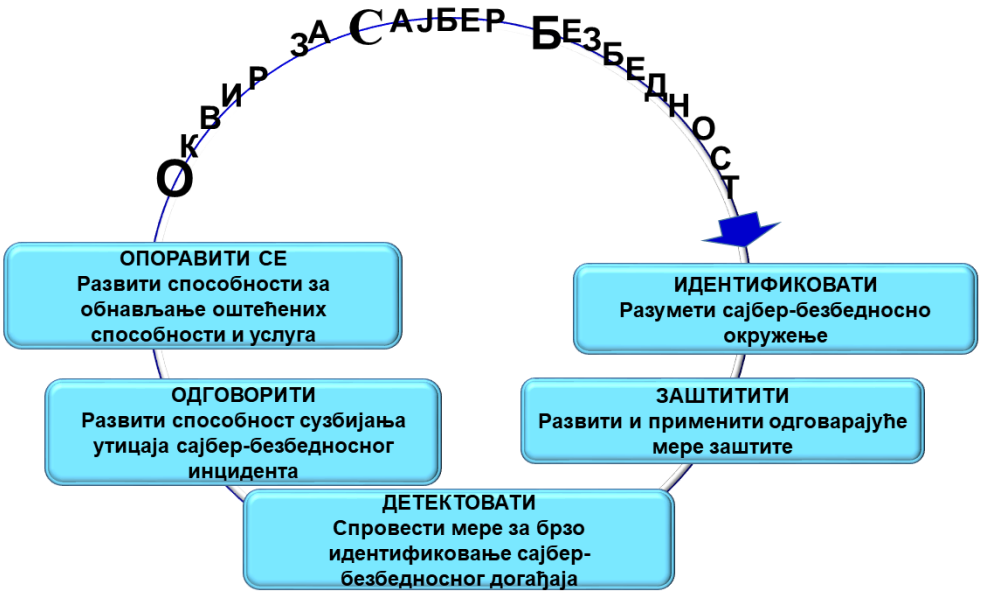
У складу с константним и растућим претњама од сајбер-напада с ″малициозним намерама, нарушавањем континуитета пословања и крађом информација″, али и ослањање сектора ваздухопловства на ″доступност система ICT, као и на интегритету и поверљивости података″, недавно успостављена стратегија ICAO, као **оквир за сајбер безбедност** који је неопходно да буде усвојена од стране авио индустрије, ослања се на следећим стубовима [217]:

- Међународна сарадња (обезбедити међународну сарадњу између држава у развоју и унапређење сајбер безбедносних решења).
- Управљање (неопходност да државе чланице укључе сајбер безбедност у своје националне програме безбедности и безбедности у ваздухопловству, као и да сарађују са својим надлежним органима за цивилно ваздухопловство како би поставили јасне стандарде управљања и одговорности за сајбер безбедност у индустрији цивилног ваздухопловства).
- Ефективно законодавство и прописи (неопходно је да државе чланице обезбеде успостављање одговарајућег законодавства и прописа за борбу против сајбер криминала и да спроводе сталну анализу како би идентификовали и

[105] ANSP – организација која пружа услуге управљања ваздухопловом у лету или у маневарски зони и која је легитимни носилац одговорности за те услуге.

модификовали све кључне законске одредбе за спречавање и кривично гоњење актера сајбер напада).

- Политика сајбер безбедности (укључивање сајбер безбедности у државне системе безбедности и надзора у ваздухопловству, и развијање оквира за управљање ризиком и политике сајбер безбедности које обухватају цео ваздухопловни систем).
- Дељење информација (неопходност свих актера авио индустрије да деле информације у вези са рањивостима, претњама, догађајима и најбољим праксама, када је то могуће).
- Управљање инцидентима и ванредним ситуацијама (препорука је успостављање планова за ванредне ситуације, како би се осигурао континуитет ваздушног саобраћаја и минимизирали поремећаји активности везаних за путнике, чак и током сајбер напада).
- Изградња капацитета, обуке и културе сајбер безбедности (да би се ојачала отпорност авио индустрије на будуће нападе, неопходно је повећати број сајбер безбедносних стручњака у сектору цивилног ваздухопловства, и неговати културу сајбер безбедности за следеће генерације ваздухопловних професионалаца).



Слика 11. Сајбер-безбедносни оквир националне инфраструктуре – механизам заштите сајбер безбедности (модификовано и преузето из [216])

С друге стране, у извештају EUROCONTROL-а (2021) [217], истиче се пораст плиме сајбер напада и изложеност европске ваздухопловне индустрије растућем нивоу ризика, јер хакери и сајбер криминалци, константно покушавају да искористе рањивости, изазову хаос и остваре финансијску добит на рачун сектора цивилне авијације и путника. Извештај, осим што анализира и пореди број и врсте пријављених сајбер инцидената, требало би и да подстакне авио-компаније и друге

заинтересоване стране у ваздухопловној индустрији да повећају мере за откривање сајбер претњи, као и за ублажавање и превенцију сајбер напада.

У стратегији (2013-2023) *Transportation Industrial Control Systems* (TICSs) *Cyber-security Standards Strategy*, од стране DHS, успостављеној 2012. године, истиче се да не постоје сајбер-безбедносни стандарди за аеродроме, а да се постојећи, углавном фокусирају на авионске контролне системе [218]. Организације које су заједнички израдиле неколико докумената за промовисање сајбер безбедносних стандарда у авио сектору су: *Airlines Electronic Engineering Committee* (AEEC), *Aircraft Information Security Subcommittee*, *Radio Technical Commission for Aeronautics* (RTCA), *Aeronautical Radio Incorporated* (ARINC) и *European Organization for Civil Aviation Equipment* (EUROCAE). Такође, у извештају EU/EUROCONTROL-а из 2016. године (SESAR *Programme*) [219], указује се на то да сајбер безбедност аеродрома и даље представља велики изазов, без обзира на примену постојеће најбоље праксе у процени и ублажавању сајбер-безбедносних претњи. Бројна безбедносно угрожена подручја, нису ограничена или лимитирана само на аеродроме, који су чворне тачке у оквиру националног и међународног ваздушног простора, као и *air-route networks.* И други делови мреже ваздушног простора, које су повезане с аеродромима, тј. критичним аеродромским операцијама, изложени су сајбер-безбедносним ризицима. Њихове кључне међусобне везе укључују размену критично-безбедносних података преко система који се заснивају на софтверу, као што су ACARS подаци, подаци о одржавању (електронски потписи, персонални подаци, резултати ревизије, итд.) У том контексту, аеродроми се могу посматрати као потенцијалне улазне тачке за сајбер претње усмерене према целом авио-систему. Ефекти сајбер напада могу имати значајне финансијске ефекте, као и последице на континуитет пословања, и с тим повезане поремећаје. Тако, увођење корумпираних или лажних података, може имати драматичне последице изван аеродрома, као нпр. на планирање лета, тј. на безбедност ATM система. Затим, потенцијално остваривање приступа системима авиона од стране сајбер преступника, с обзиром на то да многе авио-компаније, обезбеђују уграђену интернет конекцију, тј. улазну тачку за уграђене софтверске системе, и то не само оних који котролишу приступ интернету, већ и онох који су укључене у контролне и навигационе системе [220].

Различите активности сачињавају оквир за **сајбер безбедност аеродрома** , а које спроводи управа/појединци с претходно утврђеним улогама и задацима, у циљу процене и минимизирања ризика по сајбер безбедност аеродрома. Приступ се заснива на најбољим праксама, али га је неопходно прилагодити потребама сваког аеродрома, у зависности од његове величине, као и толеранције ризика и ресурса с којим располаже. Без обзира на приступ сајбер безбедности, основни циљ требало би да буде идентификовање и адресирање рањивости, како би се постигло смањење ризика на ефикасан и исплатив начин [206].

Тако, у складу са постављеним оквиром за сајбер безбедност националне инфраструктуре (сл. 11), у наставку текста ће бити укратко описане примарне активности које сачињавају механизам за заштиту сајбер безбедности аеродрома, и то: 1) идентификација, 2) заштита, 3) детекција, 4), одговор и 5) опоравак.

1) **Идентификација** – Обухвата детекцију: (а) претњи по податке и системе аеродрома – константно се повећавају по броју и софистицираности; (б) актера – хакери, државе, криминалне организације, инсајдери; (в) мотива – разлози (финансијска добит, ометање операција, итд.) због којих актери врше претње; (г) вектора – пут или канал за извршење напада; (ђ) мете – IT и ITC, као и подаци које садрже или преносе ови системи; (е) потенцијалних циљева и њихову критичност за аеродромске операције – корисници, продавци, верзије софтвера, подаци који се чувају и размењују, итд., као и процену: (а) вероватноће специфичних сајбер напада – сагледати бројне комбинације постојећих претњи, актера, вектора, мотива и циљева, (б) утицај сваке рањивости у циљу одређивања нивоа потенцијалних губитака података, или финансијског/оперативног губитка, (в) рањивости, које би требало да сумирају претње којима су изложени подаци и системи аеродрома, (г) утицај, који би успешан напад имао на податке и системе (провера рањивости може се извршти за све податке и системе, или за специфичне подскупове за које се сматра да су приоритет, тј. за хитно решавање).

2) **Заштита** – За ову активност, потребно је обезбедити: (а) новчана средства и кадровске ресурсе на основу приоритета рањивости које би требало решити, њихову толеранцију на ризик и доступност ресурса (*senior management*); (б) руковођење предузимањем противмера (*Chief Information Security Officer*), и спровођењем истих (запослени у IT сектору и особље објеката, евентуално, уз подршку спољних провајдера, на основу утврђених приоритета и додељених ресурса од стране *senior management*-а), (в) неопходне процедуре како би се осигурало адекватно успостављање и спровођење противмера; (г) адекватну политику управе аеродрома како би се осигурало поштовање спровођења процедура; (д) ажурирање система, нарочито оних који се сматрају неопходним из безбедносне перспективе (овај процес би требало аутоматизовати у највећој могућој мери; (ђ) материјал за безбедносну обуку (израдити/набавити), како би се менаџери аеродрома, особље и консултанти, информисали о њиховим одговорностима у вези са спровођењем контрамера; (е) обуку (новозапослених, и периодично свих запослених); (ж) примену најбоље праксе за примену противмера на аеродрому од стране менаџера, особља, консултаната, итд.

3) **Детекција** – Ова активност обухвата следеће: (а) сваку аномалну активност система, сумњиву људску активност и потенцијално угрожавање података, одмах саопштити особама одговорним за сајбер безбедност аеродрома (извештаје могу доставити запослени службе за помоћ или службе обезбеђења, као и менаџери); (б) надгледати мреже, преко софтвера или хардвера, а упозорења о аномалној активности, покушајима/неуобичајеним захтевима за приступ, сумњивом мрежном саобраћају/другим догађајима који могу указивати на сајбер напад, потребно је доставити одређеном особљу IT сектора, а критична упозорења, у што краћем року, *Chief Information Security Officer*-у; (в) брзо утврдити утицај пријављених активности користећи постојеће информације (прикупљене и забележене у инвентару и проценама рањивости; (г) уколико се проблем открије, одговорни за сајбер-безбедност на аеродрому, одмах би требало да предузму одговарајуће активности; (д) у складу с аеродромском комуникационом политиком, потребно је обавестити заинтересоване стране, које су претходно идентификоване као помоћ,

или које могу бити погођене сајбер нападом. При томе, потребно је одредити одговарајући садржај, време и канал(е) дистрибуције информација у вези са предузетим сајбер нападом (одговорна особа за сајбер безбедност у сарадњи са senior management-ом и особљем за комуникацију).

4) **Одговор** – У оквиру ове активности потребно је: (а) анализирати напад у циљу утврђивања озбиљности, узрока и противмера које се могу предузети – разматрати инвентар, процену ризика и метрику која квантификује стабилно нормално стање пословања; (б) спровести тријажу – коришћењем претходно дате анализе (под а), као инпута за одређивање приоритета активности, које треба предузети као реакцију на напад (акција), као нпр. гашење система, затварање мрежног саобраћаја, итд. (ове мере могу утицати на легитимне, и у неким случајевима критичне операције, требало би успоставити резервне процедуре за брзу примену, уколико је потребно); (в) уклонити узрок напада – брисањем малициозног кода, или враћањем система на последње познато стабилно стање (ова активност мора бити брза и ефикасна, јер је за њу критична примена принципа управљања конфигурацијом).

5) **Опоравак** – Ова октивност подразумева: (а) брзо враћање података и системе у њихово претходно (нормално) стање – подразумева да је претходно дефинисано нормално стање, као део процеса инвентара (активност 1) и метрика, која указује на типична оптерећења корисника и мрежног саобраћаја; (б) праћење метрике – квантификација ефекта сајбер напада и евалуација приоритетних против-мера, како би се смањила вероватноћа појаве сличних напада у будућност, као и за побољшање одговора на друге сајбер нападе.

С обзиром на јединствену међународну и симбиотичку природу ваздухопловне индустрије, као што је поменуто, борба против сајбер криминала захтева заједнички рад Владе, регулатора и учесника у ваздухопловној индустрији (део 4.1.1) на формулисању и спровођењу кохезионог плана и глобалних решења; ови ентитети/субјекти су одговорни, сваки у својој надлежности за остваривање сајбер безбедности (правна и регулативни оквир сајбер безбедности, безбедност авио-компаније и аеродрома, безбедност система ваздушне навигације, и сајбер безбедност летења). На пример, ICAO је формирала (2017) *Secretariat Study Group on Cybersecurity* (SSGC), која је, између осталог, одговорна за преглед анекса Чикашке конвенције из 1974. године, консолидацију постојећих стандарда и препоручене праксе (SARP) и разматрање предлога за измене и допуне одредби ICAO [120].

4.1.1. Правни и регулаторни оквир сајбер безбедности ваздухопловног система

Обезбеђивање сајбер безбедности ваздухопловног система, тј. ефикасно и ефективно ублажавање садашњих, као и будућих ризика од сајбер напада, или компромитовања система, у ваздухопловном сектору, може се обезбедити само партнерским односом између **Владе**, **регулатора** и **ваздухопловне индустрије** сваке државе, од којих сваки има одређене улоге и одговорности (сл. 12). То је избалансиран однос између адекватног законодавног оквира, благовремених и

тачних обавештајних података, робустног управљања ризиком, као и способности за реакцију и опоравак од сајбер инцидента уколико се исти догоди – јасно постављање улога и одговорности сваког од партнера, обезбеђује робустан приступ управљању ризиком.

Слика 12. Улоге и одговорности Владе, ваздухопловне индустрије и регулатора као партнера у успостављању сајбер безбедности (модификовано и преузето из [5])

У сектору комерцијалне авијације, неопходно је веома озбиљно разматрати сајбер ризике/претње, као и успоставити међународне споразуме о сајбер безбедности у авијацији, ако и глобалних решења [221]. Као што је дато у делу 4.1, неопходно је да авио индустрија усвоји **оквир за сајбер безбедност**, који се према *American Institute of Aeronautics and Astronautic* (AIAA) састоји из следећег: успоставити заједничке сајбер безбедносне стандарде за авио-систем, обезбедити културу сајбер безбедности, разумети сајбер претње и ризике, остварити комуникацију и имати свест о ситуацији, одговорити на сајбер инциденте, јачати одбрамбене системе, дефинисати и дизајнирати оперативне принципе, спровести неопходна истраживања и развој и обезбедити неопходну сарадњу између Влада држава и авио индустрије.

Значајна повезаност између сајбер, физичке и персоналне безбедности, захтева обезбеђивање адекватног управљања сваким од безбедносних ризика, што подразумева свеобухватан (холистички) проступ, с прецизно дефинисаним улогама сваког од партнера (Влада, авио индустрија и регулатори). Свакако, безбедност државе јесте одговорност Владе, која, у односу на ваздухопловну индустрију, располаже с много више средстава, а који укључују и приступ информацијама из обавештајних агенција. Тако, авио-сектор, ослања се на Владу, као најближег партнера, која обезбеђује информације и помаже у управљању сајбер-безбедносним ризицима, као и остваривању безбедности путника, робе и услуга.

Влада може имати кључну улогу у постављању снажног регулаторног оквира за сајбер безбедност. При томе, **Влада** идентификује критичне системе и инфраструкуре приватних, као и јавних ентитета, што, с обзиром на јаку повезаност авио-система и инфраструктуре, обезбеђује координацију између бројних агенција и приватних организација [1]. Применом модела управљања ризицима, након идентификације система од нарочитог значаја, детектују се најкритичнији системи (од стране регулатора), које је неопходно заштити. Затим, анализом претњи, утврђују се начини могуће експлоатације постојеће ICT мреже, у циљу угрожавања критичних система и инфраструктуре (IoT). Осим тога, Влада може успоставити одређене законске оквире, којима се сузбијају претње по авио-сектор у целини, и то, да контролише или дозволи продају/куповину опреме, која може представљати ризик за комуникационе системе (нпр. GNSS ометачи), радио примопредајнике и ADS–B пријемнике/предајнике, као и да се бави заштитом личних података (применом одговарајућих стандарда обезбеђује се да пакети персонализованих дигиталних услуга авио-компанија, буду сигурни и безбедни за кориснике). Поред тога, техничке сајбер безбедносне мере тако су конципиране да се супротстављају познатим претњама; међутим, због карактеристика дигиталних мрежа, реални сајбер ризици/претње, осим што су непредвидиви, и бројнији су. Због тога је неопходно да **сајбер безбедносне регулативе**, укључе и законски регулисан програм надзора, који би требало да ревидира и подржи субјекте који подлежу регулативама, затим, уведу сајбер-безбедносне политике базиране на обавезној употреби неопходних техничких мера за спречавање и откривање сајбер инцидената, вођење документације и ажурирање података, као и успостави адекватне процесе управљања сајбер инцидентима, укључујући и врло ефикасне сајбер форензичке анализе [1].

Ваздухопловна индустрија, осим што је одговорна за управљање сајбер (као и другим) ризицима својих сектора, као и испуњавање потребних регулаторних стандарда (постављених од стране Владе и Управе за цивилно ваздухопловство), потребно је и да промовише културу сајбер безбедности, као и обезбеди да сво особље (од оперативног до руководећег), има/примењује одговарајуће разумевање/знање о сајбер-безбедносним ризицима. Дакле, потребна је обука запослених, као и спровођење интерних активности контроле квалитета у циљу провере ефикасности примене сајбер-безбедносних мера. Нарочито, произвођачи софтвера и хардвера за авионске ICT, уколико је потребно (као у случају FAA и авиона *Boeing* 777) морају спровести неопходне мере за спречавање увођења нових озбиљних рањивости у оне које већ постоје. У области ATM сајбер безбедности, EUROCONTROL је објавио свеобухватни *Manual for National Air Traffic Management Security Oversight* [222]; регулатори безбедности у авијацији могу имати велику корист од имплементације ових програма надзора.

Даљем развоју авио-индустрије и применама иновативних технологија, прилагођаваће се и сајбер претње [211]. То изискује континуирану евалуацију и ревизију установљених стратегија, усклађених с променама у вези са технологијом, сајбер претњама и стандардима/регулативама, уз истиовремено подстицање регулатора да прихвате иновације.

Тако, употреба **беспилотних летилица** (*Unmanned Aerial Systems,* UAS), односно дронова[106], све је чешће, приступачније и корисније, услед већих могућности прикупљања података, као и аутономног оперативног рада, због чега је потребно изградити технолошко и регулаторно окружење које подржава ове иновације [232]. Поред техничких/механичких аспеката, посебно у фази израде прототипова дизајна беспилотних летелица/дронова, као и производње прототипова, генерално [224, 225], постоје значајни изазови сајбер безбедности у вези са овим беспилотним летелицама, а веома је важно и постојања свесности ситуације о потенцијалним тренутним/будућим радњама злонамериних актера који користе UAS у офанзивне/дефанзивне сврхе. Свакако, континуирани развој технологије и побољшане функционалности уграђене у дронове утицаће и на авио системе, као нпр. на ADS–B систем [226–228].

UAS је ″беспилотна летелица и повезани елементи (укључујући комуникационе везе и компоненте које контролишу беспилотни авион) који су неопходни да би пилот радио безбедно и ефикасно у националном систему ваздушног простора″ [229]. Дакле, UAS се сматра авионом, према одредбама међународног закона о ваздухопловству [223, 230]. Све беспилотне летелице, како оне којима се управља даљински, или потпуно аутономно, тако и оне које користе комбинацију оба управљања, подлежу Конвенцији о међународном цивилном ваздухопловству (Чикашка конвенција), а свака држава потписница обавезује се да ће осигурати да летови беспилотних авиона у регионима отвореним за цивилне ваздухоплове, буде контролисан на такав начин, да не представља било какву опасност за цивилне ваздухоплове [231]. Стога, одређене законске одредбе оквира за сајбер безбедност у ваздухопловству (прописи, стандарди, препоручене праксе, итд.) требало би примењивати и на UAS, и одговоре на евентуална питања, тј. њихова решења, тражити у овим законским одредбама [232].

С друге стране, како се претпоставља, нови развој технологије UAS, укључујући и увођење аутономнијег управљачког софтвера и могућност стварања ″роја″ дронова путем мобилних мрежа, повећавају обим и напредак потенцијалних сајбер напада (део 6.3.). Тако, ентитети који користе UAS могу бити жртве сајбер-напада, као што су они у вези с компромитовањем података, јер се ови уређаји могу контролисати са одређеног места (на земљи), где осетљиви подаци и бежичне мреже, представљају приступне тачке за злонамерним хакере.

Дакле, **сајбер нападачи**, **коришћењем UAS**, могу потенцијално експлоатисати приступне тачке, необезбеђене мреже или друге уређаје, бежично, и тако активирати злонамерни код, убацити *malware*, итд. Такође, дрон може бити хакован

[106] UAS је најчешће коришћен термин за беспилотне летилице од стране међународних организација (нпр. ICAO и EASA). Дрон је популарнији, и један од многих назива за UAS; то је и шири појам, јер се односи на шири спектар летилица, који укључују и UAS. Користе се и термини *Unmanned Aircraft* (UA), *Remotely Piloted Aircraf* (RPA), *Remotely Piloted Aviation Systems* (RPAS), *Unmanned Drones* и *Autonomous Drones*. На пример, према ICAO, RPAS је подкатегорија UAS, која се односи само на беспилотне летелице којима се управља са удаљене пилотске станице, тј. дефинише се као даљински управљани ваздухоплов с припадајућом станицом пилота, командама и контролним везама, као и осталим компонентама наведеним у дизајну датог типа RPAS [223].

употребом другог дрона, коришћењем Wi-Fi мреже. На пример, инсталирањем одређене апликације на дрон, преко отворене Wi-Fi мреже, могу се украсти подаци корисника (нпр. корисничка имена, лозинке, подаци о кредитној картици) с персоналног уређаја повезаног на мрежу [233]. Затим, могуће је да злонамерни хакер, отимањем дрона, или преузимањем контроле над дроном у току лета, потенцијално прикупи критичне податаке, што се у крајњој инстанци одражава на цивилну безбедност, као и на безбедност авиона с посадом [16]. Такође, инциденти не морају бити изведени коришћењем циљаних мрежа и система директно повезаних с UAS уређајем. Хакери могу користити, између осталог, приватну опрему оператера дронова, који се, на пример, пријављује на одређену мрежу одговорну за подешавања UAS.

Веома је важно и редовно тестирање опреме у међусекторској сарадњи (држава, приватне компаније, лабораторије, истраживачки центри и др.), јер омогућава стварање универзалних безбедносних и заштитних протокола који би могли бити имплементирани у већем обиму. При томе, кључни елемент је идентификација безбедносних ″празнина″ и предузимање ефикасних акција за њихово отклањање. С тим у вези, неопходно је стално пратити UAS системе и развој UAS технологије. Како се дронови користе у ширем спектру активности, број њихових законски регулисаних употреба ће се повећавати, али у погледу смањења ризика, један од најважнијих задатака биће разликовање и дефинисање легалних операција од незаконитих радњи коришћењем UAS.

Дакле, брзи развој UAS, као и других технологија, има безбедносне импликације, и представља изазов у погледу сигурности, безбедности и приватности, због чега је кључно разматрање сајбер безбедности од самог почетка процеса пројектовања. Без тога, повећаће се потенцијал сајбер напада, тј. способност малициозних актера да хакују UAS системе како би их користили за незаконита или као деструктивна средства. Овакав принцип мора се примењивати и на технологије следеће генерције у ваздухопловству (свемирски авиони, хиперсонични авиони, будући системи управљања ваздушним саобраћајем, итд.) – сајбер отпорност мора бити инкорпорирана од самог почетка конципирања будућих иновативних технологија.

4.1.2. Међународне организације и институције које се баве сајбер безбедношћу у авијацији

Поред националних агенција и приватних субјеката, на међународном и европском нивоу, бројне институције, агенције и конференције (ENISA, ECAC, ETSI[107], FAA, итд.), као и организације (IATA, ICAO, итд.), баве се обликовањем глобалног приступа сајбер-безбедности у авијацији; улога сваке од њих је да олакша и промовише, кроз транспарентне координисане иницијативе, развој и примену смерница и стандарда, који доприносе јачању сајбер безбедности у авијацији.

На међународном нивоу, водеће организације, одговорне за постављање регулатива уи смерница су:

[107] ETSI – *European Telecommunication Standards Institute*.

International Civil Aviation Organisation (ICAO) – поставља међународне безбедносне захтеве цивилне авијације, у облику стандарда и практичних препорука (SARPs). Такође, ICAO обезбеђује међународни оквир за решавања ″аката незаконитих сметњи″, који укључују факторе ремећења и безбедносне ефекте. Активности ове огрганизације, као једне од лидера у индустрији цивилног ваздухопловства за континуирано решавање сајбер претњи, регулисана је правним одредбама цивилног ваздухопловства према Чикашкој конвенцији (1944), основане с примарним циљем да адресира принципе међународне ваздушне навигације и помогне државама чланицама у процесу развоја међународног ваздушног саобраћаја [234]. У циљу постављања одговарајућег механизма за решавање изазова у вези с проценама стања сајбер безбедности у авио индустрији, и координисаног решавања овог задатка, ICAO (2012) је успоставила SSGC и сличне радне групе за решавање питања сајбер безбедности у цивилном ваздухопловству, тако сарађујући са државама чланицама, као и водећим заинтересованим странама у индустрији, на мапирању пута неопходних акција и развој сајбер-безбедносних одредби [120]. Као што је поменуто, ICAO је одговорна за имплементацију SARP-ова; ICAO је усвојила (2014) препоручене праксе у вези са сајбер-безбедносним мерама, као и надоградила постојећи (2018), који од држава чланица захтева да оператери и/или авио-субјекти, а према релевантној националној безбедносној документацији цивилног ваздухопловства, идентификују своје критичне информације, системе комуникационе технологије, као и податке [235]. Неопходно је да државе чланице ICAO, прилагоде националне прописе и имплементирају ICAO стандард при доношењу мера за решавање сајбер претњи.

International Air Transport Association (IATA) – међународна организација за ваздушни саобраћај, тј. међународно трговинско удружење водећих међународних путничких и карго авио-компаније (око 300) из више од 120 држава света, које обавља око 82% укупног ваздушног саобраћаја. Чланство је отворено за авио-компаније, које обављају редовне и ванредне ваздухопловне услуге, а које имају/одржавају IATA *Operational Safety Audit*. Седиште ове организације, као и ICAO, је у Монтреалу (Канада), с извршним канцеларијама у Женеви (Швајцарска). IATA подржава многе области ваздухопловних активности и помаже у формулисању индустријске политике о критичним питањима ваздухопловства – залаже се за интересе авио-компанија (поједностављивањем процеса и повећањем удобности путовања уз смањење трошкова и побољшање ефикасности), помаже авио-компанијама да раде сигурно, безбедно, ефикасно и економично, према јасно дефинисаним правилима, затим, пружа професионалну подршку свим заинтересованим странама у индустрији с широким спектром производа и стручних услуга, као и даје трословне ознаке за аеродроме (нпр. BEG за аеродром ″Никола Тесла″, Београд) и двословне ознаке за авио-компаније (нпр. JU за ″Air Srbia″, Србија). Неки од тренутних приоритета IATA [236] су у вези са заштитом животне средине (прелазак авио-компаннија на одрживо авио-гориво као приоритетну опцију за постизање нулте укупне емисије угљен-диоксида до 2050. године, као и давање подршке владама држава чланица за усвајање стратегије у вези с климатским променама), затим, повећањем безбедности (имплементацијом IATA *Safety Audit for Ground Operations*, тј. усклађених станарда релевантних за специфичне активности било ког оператера на земљи, затим, уклањањем ризика,

који су у вези са коришћењем литијумских батерија, као покретањем програма IATA *Operational Safety Audit Program*, међународно признатог и прихваћеног система евалуације дизајнираног за процену оперативног управљања и система контроле авио-компанија), као и ефикасна оперативност IATA (осигура ефикасаност *Billing and Settlement Plan*, тј. система продаје и контроле IATA акредитованих агената за продају, и побољшање финансијске контроле и тока новца, као и *Cargo Account Settlement Systems*, система који поједностављује фактурисање рачуна између авио-компанија и шпедитера, а који функционише преко CASSLink, напредног, глобалног решења за *web-enabled e*-наплату).

European Civil Aviation Conference (ECAC) – функционише као европски огранак ICAO, основана 1955. године, која је задужена за усклађивање политике и праксе цивилног ваздухопловства између држава чланица, уз промовисање/поштовање политике цивилне авијације у другим државама света. Мисија ECAC је промоција континуираног развоја безбедног, ефикасног и одрживог европског система ваздушног саобраћаја. ECAC је јединствени европски форум за дискусију о свим важнијим темама цивилног ваздухопловства, с обзиром на ECAC-ову дугогодишњу експертизу, паневропско чланство и блиске веза с ICAO, као и активну сарадњу с различитим регионалним организацијама, као и EUROCONTROL и *Joint Aviation Authorities Training Organisation* [237].

European Organisation for Civil Aviation Equipment (EUROCAE) – непрофитна међународна организација основана у Луцерну, Швајцарска (1963), која се, заједно с авио индустријом, искључиво бави стандардизацијом у цивилном ваздухопловству, како за ваздушне, тако и за земаљске системе и опрему, и то, развојем стручних кадрова и решавањем глобалних изазова у авијацији, прилагођавањем правила за употребу на међународном нивоу и подржавањем постојећих оперативних, развојних и регулативних процеса [238, 239]. Према EASA, документи EUROCAE представљају средство усклађености с заједничким техничким стандардима и другим регулаторним документима. EUROCAE је проширила своју активност и на сложене системе комуникације, навигације и надзора/управљања ваздушним саобраћајем, укључујући њихов земаљски сегмент. Одговарајућу документацију разматрају EUROCONTROL и Европска комисија, укључујући контекст Јединственог европског неба (*Single European Sky*), тј. интероперабилности Европске мреже управљања ваздушним саобраћајем.

European Union Agency for Network and Information Security (ENISA) – раније, Агенција Европске уније (EU) за мрежну и информациону безбедност (*European Union Agency for Network and Information Security*) је агенција EU, са статусом правног лица; обавља активности у вези с успостављањем високог нивоа безбедности мрежа и података у EU, подизањем свести о информационој безбедности, као и развоју и промовисању културе безбедности мрежа и података за добробит грађана, потрошача, компанија и органа цивилне власти EU. Дакле, задаци ENISA-е укључују: саветовање и помоћ државама чланицама у вези с безбедношћу информација и у њиховом дијалогу с индустријом за решавање безбедносних проблема у хардверским и софтверским производима; прикупљање и анализирање података о безбедносним инцидентима у Европи и ризицима; промовисање метода процене ризика и управљања ризиком како би се побољшала

способност за решавање проблема у вези с безбедношћу информација; подизање свести и сарадња између различитих актера у области информационе безбедности, посебно развојем јавно/приватног партнерства с индустријом. Активности агенције су груписане око четири главне теме: рачунарски тимови за решавање хитних случајева, заштита и отпорност критичне информационе инфраструктуре, идентитет и поверење, као и управљање ризиком. ENISA подржава државе чланице и друге заинтересоване стране у успостављању и примени *Computer Emergency Response Team for the EU Institutions, bodies and agencies* (CERT-EU), даје препоруке и развија најбоље праксе за агенције EU, национална регулаторна тела и приватни сектор у областима као што су национални планови за ванредне ситуације, стратегије сајбер безбедности, међусобно повезане мреже, рачунарство у облаку, итд. Такође ради на повећању поверења корисника у онлајн сервисе, као и на подржавању међусобног признавања механизама електронске идентификације и аутентификације на електронским потписима међу државама чланицама EU [240].

Federal Aviation Administration (FAA) – агенција Министарства саобраћаја USA надлежна за регулисање и надзор свих аспеката ваздушног саобраћаја у USA, с два главна центра (*Mike Monroney Aeronautical Center, Oklahoma City, Oklahoma* и *William J. Hughes Technical Center, Atlantic City, New Jersey*) и девет регионалних центара [241]. Примарна улога ове, најутицајније ваздухопловне агенције на свету, јесте осигуравање безбедности сектора цивилне авијације. Примарне одговорности FAA су регулисање цивилног ваздухопловства у циљу унапређења безбедности у USA, као и другим државама света, развој цивилног ваздухопловства, као и нових авио-система и технологија, затим, развој и управљање системом ваздушног саобраћаја и навигације за цивилне и војне авионе, као и развој и спровођење програма за контролу буке и других утицаја цивилног ваздухопловства на животну средину, итд. Истрагу ваздухопловних инцидената, несрећа и катастрофа, спроводи независна агенција Владе USA – *National Transportation Safety Board* (NTSB). FAA је, поред EASA, једна од главних агенција на међународном нивоу, одговорна за сертификацију авиона. Најважније **активности FAA**, односе се на:

- безбедносне прописе (доношење и спровођење прописа и минималних стандарда, који обухватају производњу, управљање и одржавање авиона, као и сертификација ваздухопловног особља и аеродрома који опслужују авио-превознике)
- ваздушни простор и управљање ваздушним саобраћајем (безбедно и ефикасно коришћење пловног ваздушног простора, затим, управљање мрежом аеродромских торњева, центара за контролу ваздушног саобраћаја и станица за сервисирање летова, као и развој прописа/правила ваздушног саобраћаја, центре за контролу ваздушног саобраћаја и сервисне станице, као и израду правила ваздушног саобраћаја, додељивање коришћења ваздушног простора и контролу ваздушног саобраћаја
- објекте за ваздушну навигацију (FAA гради/инсталира визуелна и електронска средства за ваздушну навигацију, затим, одржава, управља и обезбеђује квалитет ових објеката, као и одржава друге системе за подршку ваздушној навигацији и контроли ваздушног саобраћаја, укључујући опрему, радарске објекте и компјутерске системе)

- цивилно ваздухопловство ван USA (FAA промовише безбедност у ваздухопловству и подстиче цивилно ваздухопловство у иностранству, размењује информације с властима других држава, сертификује иностране сервисе, ваздухопловно особље и механичаре, даје техничку помоћ и обуку, преговара о билатералним споразумима о пловидбености с другим државама, као и учествује на међународним конференцијама)
- комерцијални свемирски саобраћај (регулише и подстиче америчку индустрију комерцијалног свемирског саобраћаја, укључујући лиценцирање комерцијалних објеката за лансирање у свемир и приватна лансирања свемирског терета са лансирних возила)
- истраживање, инжењеринг и развој (истраживање и развој система и процедура потребних за безбедан и ефикасан систем ваздушне навигације и контроле ваздушног саобраћаја, затим, развој бољих авиона, мотора и опреме и тестира/процењује ваздухопловне системе, уређаје, материјале и процедуре, као и бави се аеромедицинским истраживањима)
- ATM (FAA има комплексан сет одговорности у области ATM-а и обезбеђује све главне аеродромске објекте; у оквиру регулаторног одељења FAA основана је организација за надзор безбедности ATM-а која је одговорна за надзор безбедности операција и активности ATO-а.

Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) – тим за превенирање сајбер безбедносних ризика у институцијама, органима и организацијама EU; сарађује са CERT-овима држава чланица EU и агенцијама специјализованим за сајбер безбедност.

Ваздухопловство је јединствена критична национална инфраструктура која, у односу на класичну (електронску), захтева примену виших безбедносних стандарда за заштиту својих система од сајбер напада. Због тога је постављање законских оквира у вези са сајбер безбедношћу од изузетног значаја – процес је у почетној фази, али су покренути значајни напори на међународном, регионалном и националном нивоу за решавање проблема. Лидер у томе јесте ICAO, која је још 70.-их година 20. века објавила *Security Manual*, као помоћ државама чланицама у вези са предузимањем мера за спречавање незаконитог деловања, његовог минимизирања, као и постављањем стандарда, усвајањем анекса 17 Чикашке конвенције, чиме су постављени темељи безбедносне културе. Затим, ICAO је направила први корак напред [6] у идентификацији потенцијалних сајбер-безбедносних ризика (2001), тако што је започела програм ревизије контроле приступа и сличних безбедносних пропуста у ICT системима (*Universal Security Audit Programme* [242]. У годинама након тога, ICAO је ефективно ојачала постојеће SARP-ове, и развила нове практичне безбедносне стратегије, које се односе на авионске интерент мреже. Радна група за интернет инжењеринг (*Internet Engineering Task Force*, IETF), Интернет корпорација за додељивање имена и бројева (*Internet Corporation for Assigned Names and Numbers*, ICANN), FAA и EUROCONTROL, заједно са ICAO (2008), анализирали су утицај *Boeing*-овог *"Connexion"* сервиса *(in-flight online internet connectivity service)* (фуснота 64) на глобални интернет.

Концепт према коме је одговорност за било какво кршење безбедности у ваздухопловству одговорност сваке државе (с обзиром на то да су телекомуникације национални субјект), дугорочно је неодржив, уколико се узме у обзир свеприсутност коришћења интернета – огроман број авиона ће користити сопствене интернет базе при чему свака држава поседује и контролише своје мрежне операције, уместо идеалног јединственог мрежног оператера. У том смислу, идеално би било да ICAO дефинише „затворену/изоловану“ мрежну архитектуру, која би омогућила једноставније управљање и изоловање мреже, али то се, још увек, чини далеким [6].

Такође, ICAO улаже велике напоре на успостављање нових безбедносних стандарда за **системе беспилотних летилица** (UAS)[108], а како су ови системи изложенији сајбер нападима, детаљно разматрање сајбер-безбедносних питања UAS, може бити од великог значаја и за генералну авијацију. ICAO континуирано ради на развијању регулаторног оквира и најбоље праксе за UAS, који се могу применити на глобалном нивоу [244], као помоћ државама у имплементацији/допуни националних прописа за операције својих несертификованих UAS. Дизајн новог модела прописа (засновани на значајним акумулираним безбедносним подацима, проширеним принципима управљања безбедношћу који су генерисани и унапређени последњих година у комбинацији с алатима за доношење одлука заснованим на ризику), обезбеђује флексибилност у погледу садржаја и нивоа толеранције ризика, тако дајући државама и регулаторима међународно усклађен материјал, заснован на најновијим достигнућима, тј. пратећи развој и напредак UAS технологије. При томе, државе могу усвојити модел прописа у целости, или изабрати неке од одредби, као допуну постојећих националних UAS оквира. Свакако, редовно ажурирање ових прописа, обезбеђује усаглашеност између развоја националних UAS програма, и економске и друштвене користи примене UAS [245]. Дакле, у циљу успостављања основа за безбедну, сигурну и одрживу интеграцију беспилотне авијације у глобални систем ваздушног саобраћаја, као што је претходно истакнуто, ICAO покреће/спроводи бројне координисане активности, које укључују широк спектар ваздухопловних области (услуге ваздушне навигације и економију аеродрома, укључујући идентификацију механизама за надокнаду трошкова за пружање услуга ваздушне навигације UAS-у, екологије, тј. проблема буке, итд.). Затим, бројне су активности, које ICAO преузима у вези са UAS, као нпр. бави се безбедносним питањима везаним за незаконити употребу UAS (у сарадњи с Канцеларијом UN за борбу против тероризма и другим ентитетима), затим, ICAO у сарадњи с *United Nations International Children's Emergency Fund* (UNICEF), подржава ефикасну примену UAS у хуманитарне и развојне сврхе, као и даје смернице државама у којима UNICEF има своје активности, итд.

У области цивилне авијације, разматрањем нових сајбер ризика, на иницијативу ECAC-а (2009), предлог *Committee on Unlawful Interference* и препорука *Aviation*

[108] Очекује се да ће глобално тржиште транспорта и логистике подржано UAS-ом, порасти с 11 милијарди US долара (2022) на 29 милијарди US долара (до 2027), као и да ће број произведених UAS (2030) бити око 6,5 милиона. Тако ће, тржиште цивилних беспилотних летелица бити један од сектора с најдинамичнијим растом у наредној деценији [243].

Security Panel's, донета је одредба према којој, свака држава, потписница, мора развијати безбедносне мере за заштиту ICT система, који се користе у цивилној авијацији, од ризика или сметњи, а које могу угрозити безбедност цивилне авијације. Иако је дата као препорука, неопходност решавања питања у вези са сајбер безбедношћу, може приморати државе да предузму напоре у том смеру.

У вези с решавањем питања **сајбер тероризма**, први корак била је Пекиншка конвенција (2010), према којој је додатно криминализован акт употребе цивилног ваздухопловства као оружја, као и напади на објекте ваздухопловне навигације, ометање њихових операција и/или преношења лажних информација [244]. У авијацији, за доношење закона и прописа у вези са сајбер безбедношћу, од значаја су препоруке и успостављени механизми за решавање безбедносних питања у примени ICT, а којима се баве различите међународне и европске организације, као што су *United Nations* (UN), *Council of Europe*, *Interpol*, ECAC, итд. Према конвенцији о **сајбер криминалу** (2001) [6], у вези са ситуацијом у којој се сајбер технологија може користити за извршење кривничних дела, препоручује се државама потписницима конвенције, да усвоје законодавне и друге мере за сузбијање незаконитих сајбер активности, као што су незаконити приступ подацима, пресретање података или њихове размене, незаконито коришћење уређаја, програма и лозинки и сл. На ово се наслањају различите стратегије и споразуми о сарадњи, усвојене од стране EU, *Association of Southeast Asian Nations*, *International Telecommunications Union, Economic Community of West African States*, итд. Развој у регулисању сајбер активности на међународном нивоу био је нацрт споразума UN (2014) о оснивању Међународног кривичног суда/Трибунала за сајбер простор, као темељ за успостављање јаког и јединственог механизама за кривично гоњење извршиоца сајбер-напада на сектор авијације [246].

Свакако, од велике важности су **национални закони**, које су неке државе усвојиле у складу с Конвенцијом о сајбер криминалу. Међутим, ефикасност ових закона је под знаком питања – међу многобројним одредбама у вези са надлежностима, приватности података, интернет садржајима и сл., одредбе, које се односе на сајбер безбедност, или не постоје, или су неадекватне (нпр. казне за сајбер преступе непропорционалне су финансијском губитку, који проузрокују) [6]. Генерално, недостаци се односе на неразумевање концепта сајбер криминала, и то нарочито, недостатак дефинисања одредница, као што су хаковање, незаконито ометање, пресретање, итд. На пример, у Индији, казна за злонамерно хаковање је затворска (три године) или новчана (1.000 €), док се у Кореји, за било коју штету нанету критичној информационој структури, добија затворска казна (десет година) или новчана (100 милиона корејских вона) [6]. Сигурно је да ће пораст сајбер инцидената, приморати многе државе да еволуирају своје националне законе у вези са сајбер безбедношћу, и тако их прилагоде постојећој ситуацији и захтевима.

Поред закона, различите **смернице и добре праксе** у вези са мерама контроле сајбер безбедности, често, у оквиру ваздухопловних упутстава, прописују различите организације, као што су нпр. IATA приручник за сајбер безбедност у авијацији, ECAC смернице о мерама контроле сајбер безбедности, као и истраживања EUROCONTROL-а у различитим фазама програма *Single European Sky*. Тако, *Centre for Protection of National Infrastructure* (UK), *National Institute of*

Standards and Technology (USA), и неколико других регионалних организација, истичу важност питања контроле сајбер безбедности и добијања координисаног и ефективног одговора. Као што је претходно поменуто, FAA је лидер у анализи свих аспеката сајбер-безбедности. Ова организација је (2015), делегирала *Advisory committee* за давање препорука у вези са *Aircraft Systems Information Security/ Protection* (ASISP). Затим, развијају се *Airborne Radio Standards,* као и дају смернице за стандардизацију авио-ICT компонената. FAA сарађује с US *Homeland Security* у процесима процене и управљања сајбер безбедносним ризицима, а предлози FAA могу бити архетип будућих прописа и закона, који правно регулишу сајбер безбедност у ваздухопловству. Тако је покренута ревизија (2018) фокусирана на активности *Aviation Cybersecurity Initiative* (ACI)[109], као и улогу и одговорности FAA, као члана ACI. Циљ ове ревизије био је да испита улоге, одговорности и поступке FAA, и то нарочито оних у вези са надлежностима FAA у сектору цивилне авијације и управљању ваздушним саобраћајем, а у вези с чланом 2111 Закона о FAA *Extension, Safety, and Security* (2016), који захтева да FAA развије свеобухватан и стратешки оквир принципа и политике смањења сајбер-безбедносних ризика у систему ваздушног саобраћаја.

Осим поменутих институција, организација и агенција, у истраживања сајбер рањивости цивилне авијације, као и давању препорука и смерница заинтересованима, активно учествују и независни сајбер безбедносни аналитичари, универзитетске ICT лабораторије, као и етички хакери [143]. Свакако, свеобухватан приступ проблему, налажење решења и примена добре праксе, може бити једини начин за успостављање снажне и јединствене архитектуре сајбер безбедности у ваздухопловству. Такође, у циљу обезбеђивања ефикасне заштите и регулисања различитих заинтересованих страна, неопходна је евалуација одређених регулатива и закона, да би се исти ускладили са реалном ситуацијом, тј. растућим бројем сајбер-зависних система.

4.1.3. Сајбер безбедност у Европској Унији и Србији

Стратегије за процес заштите сајбер простора од нежељене употребе/било ког облика угрожавања, који може имати штетне последице по податке/програме/процесе у рачунарским мрежама, тј. стратегије за обезбеђење сајбер простора, дају оквир за организовање и утврђивање приоритета, као и смањење рањивости критичних информационих инфраструктура [33] њихова имплементација, веома доприноси повећању безбедности у сајбер простору.

Европска унија би требало да заштити *on-line* окружење, које омогућава максималну могућу слободу и сигурност за добробит свих. Иако је превасходно задатак сваке држава чланица EU да се индивидуално суочава с бедносним изазовима у сајбер простору, стратегија EU предлаже конкретне акције (краткорочне и дугорочне), које укључују различите политичке инструменте, као и

[109] ACI је међуагенцијска радна група FAA-а, DHS-а и DOD-а (*Department of Defense*), чији је циљ идентификација и ублажавање сајбер претњи на системе, који утичу на авио индустрију и јавност [247].

врсте актера (институције EU, државе чланице или индустрија), а које могу побољшати укупни учинак EU у вези са сајбер безбедношћу.

Визија EU у стратегији (2013) артикулисана је у следећим стратешким приоритетима: (а) постизање сајбер отпорности, тј. обезбеђивање еластичности (способност система да се аутоматски врати у претходно ″нормално″ стање након инцидента); (б) драстично смањење сајбер криминала; (в) развој политике сајбер одбране и капацитета у складу с *Common Security and Defence Policy* (CSDP)[110]; (г) развој индустријских и технолошких ресурса за сајбер безбедност; (д) успостављање кохерентну међународну политику сајбер простора за EU и промовисати основне вредности EU [91, 248].

Почевши од ове **стратегије сајбер безбедности**, EU је развила кохерентну и холистичку међународну сајбер политику [249]. Радећи са својим партнерима на билатералном, регионалном и међународном нивоу, EU је промовисала глобални, отворен, стабилан и безбедан сајбер простор, уз уважавање основних вредности EU, заснован на владавини права. Штавише, EU је била подршка ″трећим земљама″ у повећању сајбер отпорности и способности да се ове државе суоче са сајбер криминалом. Такође, EU је постигла значајан напредак у сарадњи у области сајбер одбране, нарочито у области CSDP, као и у контексту *Permanent Structured Cooperation* (PESCO) и рада *European Defence Agency*.

Нова статегија сајбер безбедности EU је одговор на изазове геополитичке конкуренције у сајбер простору и порасту сајбер претњи, нарочито након пандемије *Covid*-19, омогућавајући EU да повећа своју отпорност и буде лидер у сајбер простору, изгради капацитете за спречавање, одвраћање и реаговање на сајбер нападе, као и ојача партнерство у корист глобалног и отвореног сајбер простора.

Тако, **нова стратегија сајбер безбедности EU** обухвата следеће приоритетне активности, с бројним конкретним предлозима, који доприносе снажној EU у сајбер простору [249]:

- јачање међународне безбедности како би се допринело одговорном понашању државе у сајбер простору
- јачање алата за сајбер дипломатију EU за спречавање, одвраћање и реаговање на сајбер нападе
- јачање координације и сарадње у области сајбер одбране и изградња капацитета за сајбер одбрану
- јачање и ширење међународног партнерства и размене информација с међународним организацијама, партнерским државама и цивилним друштвом, као и академским круговима и приватним сектором
- повећање обима, ефективности и ефикасности екстерне изградње сајбер капацитета EU.

Такође, EU у оквиру сајбер безбедносне стратегије сугерише на неопходност постојања **правно регулисаних аката**, и то у вези с:

[110] *Common Security and Defence Policy* (CSDP) – Заједничка безбедносна и одбрамбена политика.

- успостављањем заједничких минималних захтева за мрежну и информациону безбедност – успостављање компетентних ауторитета за мрежну и информациону безбедност на нивоу држава и функционалног CERT-а, као и усвајање националне стратегије и националног кооперационог плана за безбедност мрежа и информација, што је све обавезујуће за државе чланице EU
- развојем и успостављањем адекватног механизма за координисано превенирање, детекцију, ублажавање и одговора на сајбер нападе, као и размену информација и сарадњу/подршку између националних компетентних ауторитета за безбедност мрежа и информација
- проактивним учешћем приватног сектора.

EU унапређује законске оквире за јачање безбедносних захтева у вези са свим дигиталним хардверским и софтверским производима. Предложени закон, под називом *Cyber Resilience Act*, обухватао би све такве производе, од рачунара и мобилних телефона до паметних кухињских апарата и дигиталних дечијих играчака, тј. личних уређаја који су повезани на интернет (IoT) [250]. Према предложеном закону[111], неопходно је да се IoT[112] дизајнирају, развијају и производе на начин који ублажава сајбер-безбедносне ризике (нпр. захтеве за продају производа, који су безбедне конфигурације, одржавање фундаменталног система идентификације производа, као и могућност решавања рањивости путем безбедносних ажурирања).

Поред **Закона о сајбер отпорности** (*Cyber Resilience Act*), донето је и неколико других закона предложених широм света[113], који имају за циљ сузбијање сајбер криминала, а који је коштао глобалну економију 5,5 билиона евра у 2021. години (очекује се да ће до 2025. године финансијска штета од сајбер криминала бити већа од 10 билиона евра). Овај закон би требало да обезбеди да конектовани објекти и софтвер који се купује на јединственом тржишту EU, буду усклађени с јаким сајбер-безбедносним мерама заштите. Такође, очекује се да ће ојачани протоколи за сајбер безбедност помоћи компанијама и произвођачима – посебно мањим предузећима која можда немају техничке ресурсе или финансијска средства да ″преживе″ сајбер напад. На крају, у вези са сајбер безбедношћу, Европа је јака онолико колико је јака њена најслабија карика: било да се ради о рањивој држави чланици или небезбедном производу дуж ланца снабдевања. Лидери у производњи, компаније и

---

[111] Овај закон је први пут представила председница Европске комисије Урсула фон дер Лајен у новембру 2021. Уколико га одобре Европски парламент и Европски савет, државе чланице EU ће морати, у наредне две године, да се адекватно прилагоде одредницама овог закона.

[112] На пример, напади *ransomware*-а се дешавају широм света сваких 11 секунди и коштали су глобалну економију око 20 милијарди евра (2020), док су DDoS напади коштали економију EU око 65 милијарди евра у 2020. години [250].

[113] У USA је 2022. године, донет нови закон којим се пооштравају захтеви за откривање сајбер криминала компанија, које припадају секторима критичне инфраструктуре. Разлог је био веома јак напад *ransomware*-а (2021) на *Colonial Pipeline*, који управља највећим националним системом цевовода за бензин, млазно и дизел гориво. Напад, који је наводно покренут преко старе корпоративне виртуелне приватне мреже, паралисао је цевоводе широм источне обале USA и резултирао тиме да је *Colonial Pipeline* исплатио хакерима биткоине у вредности од око 5 милиона долара. Америчко министарство правде је касније вратило скоро половину исплаћене откупнине [250].

њихови управни одбори, требало би да обрате пажњу на то да је развој сајбер стратегија, део пословне стратегије, као и да је разумевање сајбер ризика део доброг управљања у дигиталном добу.

Према директиви Европског парламента и Савета о мерама за осигурање високог заједничког нивоа мрежне и информационе безбедности у EU, **државе чланице EU**, неопходно је да **успоставе**:

- националну стратегију и кооперациони план за мрежну и информациону безбедност
- национални компетентни ауторитет[114] за националну стратегију за безбедност мрежа и информација
- национални CERT.

Најважније институције EU из области безбедности мрежа и информација су **ENISA** и **CERT-EU**. Њихове надлежности и задаци описани су у делу 4.1.2. ENISA, као орган EU са статусом правног лица, основана је 2004. године, уредбом (бр. 460/2004) Европске комисије и Савета, с ограниченим мандатом, који је на предлог Европске комисије, два пута продужаван. Уредбом су успостављени органи ENISA (Управни и извршни одбор, извршни директор и стално тело заинтересованих страна), њихов делокруг рада, састав, као и избор и трајање мандата. Извршни директор ENISA припрема нацрте програма пословања (које разматра и усваја Управни одбор); њему се упућују и захтеви за савете и подршку (подносиоци могу бити европски парламент, Савет, европска комисија или надлежна регулаторна тела држава чланица EU, као што су она дефинисана чланом 2. Директиве бр. 2002/21/EC у вези са заједничким правним оквиром за електронске комуникационе мреже и сервисе), који након поднетог захтева и потенцијалних активностима по захтеву, обавештава Управни и Извршни одбор. Буџет ENISA сачињавају средства EU, донације држава чланица EU, као и трећих земаља, које учествују у раду ENISA; буџет усваја Управни одбор по спроведеној процедури, која је утврђена Уредбом. Ова Уредба, тј. правни акт, веома је значајан, јер успоставља орган с којим Република Србија (RS), као држава приступница EU, за сада, треба да оствари сарадњу. У случају RS, уредба није акт директне хармонизације, тако да се не може разматрати њена усаглашеност с правним актима RS; уредба ће се директно и непосредно примењивати на RS, када наша држава постане пуноправни члан EU.

У Републици Србији, стратегија развоја информационог друштва и информационе безбедности за период 2021–2026. године, коју је усвојила **Влада RS**, представља међусекторску стратегију којом се утврђују циљеви и мере за развој информационог друштва и информационе безбедности, као и утврђује визија развоја информационог друштва у наредних пет година, дефинисањем кључних мера и активности [251, 252]. Део стратегије који се односи на информациону безбедност, усклађен је с Директивом о мрежној и информационој безбедности EU

[114] Национални компетентни ауторитет је најзначајнија институција на нивоу државе, са следећим обавезама: прати примене Директиве на националном нивоу, сарађује с националним компетентним ауторитетима држава чланица EU и с безбедносним службама, као и националним ауторитетима за заштиту података, као и прима обавештења и преузима активности након пријема обавештења о инциденту код јавне администрације и оператера телекомуникационих и информационих услуга.

(*Network and Information Security Directive*), према којој је обавеза држава да успоставе националну стратегију за информациону безбедност с дефинисаним стратешким циљевима и приоритетима у вези с мрежном и информационом безбедношћу. За израду стратегије релевантна су планска и стратешка документа у различитим областима (нпр. развој мрежа нове генерације, вештачке интелигенције, индустријске политике, правосуђа и високотехнолошког криминала, и сл.) као и прописи у области електронског документа, електронске идентификације и услуга од поверења, информационе безбедности, и сл. У вези са информационом безбедношћу ICT система од посебног значаја, неопходност адекватне заштите ICT система јесте премиса националног Закона, а што подразумева примену техничких, организационих и кадровским мера, као и других законских обавеза, а које се односе на пријаву инцидената, достављање статистичких података, редовну ревизију ICT, итд. Законом, као и пратећим подзаконским актима уређују се следеће области: дефинисани ICT системи од посебног значаја, као и мере заштите ICT система од посебног значаја; образовано Тело за координацију информационе безбедности; успостављен Национални CERT, CERT органа власти и CERT-ови самосталних оператори ICT система; дефинисана листа инцидената који значајно угрожавају информациону безбедност и обавеза пријаве инцидената; успостављена инспекција за информациону безбедност; уређена крипто-безбедност и заштита од компромитујућег електромагнетног зрачења; предвиђена могућност успостављања и евидентирања посебних CERT-ова.

Институције RS активно учествују, кроз билатералну сарадњу, или сарадњу с различитим међународним организацијама (UN, Организације за европску безбедност и сарадњу, Међународну унију за телекомуникације, Глобални форум за сајбер експертизу[115], Женевски центар за управљање сектором безбедности[116], итд.) у међународним активностима у области информационе безбедности. RS је имала (2016–2017. године) пун мандат у UN Групи владиних експерата задужених за развој у области информација и телекомуникација у контексту међународне

[115] RS је чланица *Global Forum of Cyber Expertise* (GFCE) од 2019. године. Улога GFCE је јачање међународне сарадње у изградњи сајбер капацитета, повезујући потребе, ресурсе и стручност, као и доступност практичних знања глобалној заједници. Тренутни фокус GFCE је координација регионалних и глобалних пројеката и иницијатива за сајбер капацитете, дељење знања и стручности (препоручивањем алата и публикација), затим, усклађивање индивидуалних потреба за сајбер капацитетима с понуђеним мерама подршке, као и прикупљање и одређивање приоритета истраживачких ″празнина″ у глобалној истраживачкој агенди за изградњу сајбер капацитета. GFCE је и платформа за дискусију на високом нивоу, организовање двогодишњих састанака за процену напретка и одржавање политичких дискусија о начинима и средствима одговора на нове изазове у домену изградње сајбер капацитета, а GFCE догађаји са више заинтересованих страна доприносе развоју најбољих пракси, и стога имају додатну вредност за ширу заједницу у изградњи сајбер капацитета на глобалном нивоу [253].

[116] У реализацији пројекта Женевског центра за управљање сектором безбедности ″Унапређење управљања сајбер безбедношћу на Западном Балкану″ (започео 2018. године), учествују Министарство трговине, туризма и телекомуникација, Министарство унутрашњих послова и Национални CERT RS, који би требало да допринесе ефикаснијем и одговорнијем управљању сајбер безбедношћу на Западном Балкану, као и да унапреди регионалну сарадњу у овој области [251].

безбедности (*United Nations Group of Governmental Experts*, UN GGE); RS је чланица UN Отворене радне групе за питања информационе безбедности (UN *Open-Ended Working Group*) [254], од њеног оснивања (2018), и активно учествује у раду Групе. Поред тога, Министарство спољних послова RS, као један од носилаца активности у вези с развојем међународне сарадње у области информационе безбедности, планирања и реализације билатералних контаката у циљу промоције и унапређења сарадње с другим државама, разматра све иницијативе од значаја за информациону безбедност на националном и глобалном нивоу. Тако, RS је подржала и планира активно учешће (за сада као члан радне групе) у иницијативи Француске, *"Paris Call for Trust and Security in Cyberspace"*[251]. Затим, **RS активно учествује** у раду неформалне радне групе за сајбер безбедност (*Informal Working Group on Cyber Security Issues*), основане одлуком *Organization for Security and Cooperation in Europe* (OSCE)[117], бр. 1039, тако да је RS спонзорисала *Мере за изградњу поверења број 9* (односи се на израду листе националне терминологије и дефиниције термина у области информационе безбедности), што је резултирало израдом платформе која садржи више од 1000 термина и дефиниција преузетих из легислативе држава чланица.

И други пројекти, који се спроводе у нашој држави, као што је Меморандум о разумевању о сарадњи у јачању информационе безбедности RS (закључен 2019. године, између *United Nations Office for Project Services*[118], Министарства трговине, туризма и телекомуникација RS, Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ) и Амбасаде Краљевине Норвешке у Београду), имају за циљ подршку стратешком и регулативном оквиру у области информационе безбедности, као и набавци и постављању платформе за спровођење вежби из информационе безбедности у РАТЕЛ-у. Такође, Министарство одбране RS континуирано учествује у међународним војним вежбама, као нпр. вежбе „Сајбер Тесла", која се реализује у сарадњи са јавним и приватним сектором RS који имају надлежност у области информационе безбедности и припадницима Националне Гарде Охаја (USA).

Као и било где у свету, и у **ваздушном простору RS**, постоје потенцијално опасне ситуације за ваздухопловство, тј. ситуације које могу имати/изазвати негативне ефекте по ваздухопловство, и које могу бити проглашене кризним, а које карактерише неочекиваност, необична природа, велика распрострањеност, брзина

---

[117] Појава нових безбедносних изазова у све нестабилнијем међународном окружењу представља нове ризике за OSCE. Ипак, OSCE-ов концепт свеобухватне безбедности наставља да буде релевантан за решавање оваквих изазова, како унутар OSCE-овог подручја деловања, тако и партнерских медитеранских и азијских држава. Нови безбедносни изазови су међудимензионалне ризици и претње од дигиталне технологије, борба против злочина из мржње на друштвеним мрежама, затим, веза између климатских промена, развоја и безбедности [255], као и миграције и трговина људима, као и пандемије COVID-19 [256].

[118] *United Nations Office for Project Services* (UNOPS) – Канцеларија UN за пројектне услуге, лоцирана у Копенхагену (Данска), је оперативни огранак UN, који подржава успешну имплементацију пројеката изградње мира, хуманитарних и развојних пројеката у више од 100 држава света; активности UNOPS су нпр. подршка у реаговању на Covid-19, реформи сектора безбедности, инфраструктура физичког обезбеђења, развоју националних капацитета и саветодавних услуга [257].

догађаја, итд. При томе, ескалација поремећаја од потенцијалног и/или актуелног стања до нивоа кризе, зависи од обима/ширине догађаја. Према *European Aviation Crisis Coordination Cell* (EACCC) *Rules of Procedure* [258] неке од кризних ситуација су: дисперзија вулканског пепала (*Volcanic ash dispersion*), нуклеарних честица (*Nuclear emissions dispersion*) и токсичних хемикалија (*Hazardous chemicals dispersion*), опасне метеоролошке појаве (*Heavy meteorological conditions*), претња из свемира (*Threat from space*), распростирање болести ваздушним саобраћајем (*Airborne spread of diseases*), пандемије (нпр. COVID-19), пожар (*Fire*), штрајк неколико ANSP (*Industrial action of several ANSPs*), дуготрајни поремећај (*Perturbation of a long duration*), већи поремећај пан-европских функција (*Major failure of a pan-European function*), претње у вези с обезбеђивањем (*Security threats*) и сајбер напад (*Cyber Attack*). Свакако, за превенирање узрока опасних ситуација у ваздухопловству, као и оних који могу из њих произићи, дефинисане су процедуре у кризним ситуацијама, од стране бројних организација. У Европи су то *Eurocontrol Network Manager*, EACCC, *State Focal Point* (SFP)[119], *EU Humanitarian Aid and Civil Protection department*), итд. Иницијативе за превенцију кризних ситуација подразумевају развијање безбедносних процедура, одржавање састанака, спровођење вежби симулације неких од опасних ситуација (нпр. сајбер напад) и едукацију запослених у ваздухопловству. У Србији, Директорат цивилног ваздухопловства RS (у даљем тексту Директорат) [259] активно учествује у раду ових европских организација и тела. Директорат следи националне, као и међународне прописе из области кризних ситуација, обавља консулатације с релевантним телима и организацијама (*Network Manager* (NM), EACCC, EASA, ICAO, SFP других држава), као и учествује у неким вежбама, организованим на националном и међународном нивоу.

Тако, RS је учествовала у вежби VOLCEX18 (2018) и одржала регионалну вежбу SIGMET *Coordination* [260]. Међународна вежба ICAO, VOLCEX18 под лидерством ISAVIA *(Icelandic Civil Aviation Administration)* и EUROCONTROL/NM је била симулација кризне ситуације – распршивање вулканског пепала (*Volcanic ash dispersion*), тј. симулација ерупције вулкана *Öræfajokull* на Исланду, и утицаја облака вулканског пепла на велики део Европе, Северног Атлантика и источног дела Северне Америке (и претходних година, 2012. и 2014. године, RS је успешно учествовала у сличним вежбама). Директорат се преко свог ASFP (*Alternate State Focal Point*) у сарадњи с AirSERBIA (ERT, NOC), SMATSA MET, NOF и ACC/FMP, припремио за вежбу, а након што је иста одржана, закључено је да су остварени главни циљеви вежбе – проверене и усаглашене све комуникационе везе (националне и међународне), затим, проверене и усаглашене све процедуре и поступци, као и уочени пропусти и инкорпорирана побољшања у припрему за потенцијалну реалну опасност овог типа кризне ситуације. Поред тога, Директорат је учествовао у редовној годишњој радионици *EASSS* 2018 у Бриселу, организоване од стране EUROCONTROL-а, на којој су, поред сталних чланова EACCC (представници EUROCONTROL-а), били и представници Европске комисије, EASA, IATA, затим, представници ICAO програма CAPSCA (*The Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil*

[119] SFP (*State Focal Point*) – национална контакт особа за кризне ситуације.

Aviation), као и бројни SFP. Једна од важних тема радионице, била је анализа регистра ризика опасних појава, као што су сајбер напад, оружани сукоби, нуклеарне катастрофе, и сл., а што би требало да буде основа за креирање националних регистара држава.

Такође, Директорат даје генералне смернице субјектима, који могу бити од значајни за предузимање одређених активности у кризним/опасним ситуацијама у ваздушном простору RS [259] – израђује процедуре и упутства за поступање и смањење ризика, у различитим опасним/кризним ситуацијама, затим, обезбеђује спровођење координисаних поступака свих потенцијалних субјеката и њихов редован тренинг, као и врши све друге припремне активности, које могу бити од значаја за потенцијално опасну/кризну ситуацију.[120] При свему овоме, постојање/непостојање упутства за реаговање на неку опасну/кризну ситуацију, субјекта не ослобађа од неопходности поштовања последње важеће међународне и националне регулативе, стандарда и препорука за конкретне опасне ситуације.

Кризне ситуације, а с обзиром на њихове карактеристике, захтевају одлуке, које су квалификоване и брзе. Одлука – подизање нивоа опасне ситуације на ниво кризне ситуације, по правилу, доноси се процесом заједничког одлучивања најрелевантнијих учесника (*Cooperative Decision Making process* – CDM). У Европи, за координацију овог процеса, одговоран је NM/EACCC, а у RS, процес је координисан од стране Директората, тј. SFP.

Дакле, одговорност Директората је доношење и објављивање докумената и упутстава за поступање у вези с различитим опасним ситуацијама у ваздухопловству, које потенцијално могу довести до кризних/опасних ситуација, и то: генерални приступ, врсте, обим, фазе и друго од значаја за опасне ситуације, општа упутства за поступање субјеката, који су значајни за предузимање активности у опасним ситуацијама у RS, као и поступање Директората. У ванредним ситуацијама [121] у ваздухопловству, Директорат поступа у складу са генералним приступом RS у случају ванредних ситуација и јединственим системом заштите и спасавања, које се заснивају на Националној стратегији и Националном плану заштите и спасавања у ванредним ситуацијама [261, 262]. Влада RS формира оперативно-стручно тело, Републички штаб за ванредне ситуације (у оквиру Министарства унутрашњих послова) које је одговорно за координацију и руковођење заштитом и спасавањем у ванредним ситуацијама, као и спровођење Закона о ванредним ситуацијама. Између овог штаба и Директората, оперативна веза јесте именована особа, тј. SFP, најчешће из менаџмента Директората. SFP-у се делегирају активности и одговорности Директората у вези с управљањем опасним/кризним ситуацијама у ваздухопловству. Како је SFP истовремено и члан EACCC, тако да је SFP спона Директората и EACCC, али и са свим другим

[120] Више о овоме видети у [259].

[121] Ванредна ситуација је стање у коме су ризици и претње последице опасних догађаја (катастрофе, ванредни догађаји или друге опасности по људе, животну средину или материјална добра) таквог обима и интензитета, да се њихов настанак или последице не могу пречити или отклонити редовним активностима надлежних органа/служби, већ се, за њихово ублажавање или отклањање, морају употребити посебне мере, снаге и средства уз појачан режим рада [261].

субјектима на националном и међународном нивоу, који су од важности за предузимање активности у конкретној/реалној опасној ситуацији [259].

4.2. МЕТОДОЛОГИЈА ПРОЦЕНЕ САЈБЕР БЕЗБЕДНОСТИ

Проблеми сајбер безбедности, према ICAO [235] могу се решити преко *Safety Management System*-а (SMS).[122] Према FAA [264], **ефикасан SMS** укључује компоненте, које се ослањају једне на друге, и то су:

- безбедносна политика
- управљање безбедносним ризиком
- осигурање безбедности
- промоција безбедности

Ниво до кога се остварују сваки од ових активности/компоненти, зависи од интерног и екстерног контекста у којем функционише SMS. **Безбедносна политика**, односи се на документоване стандарде (смернице и процедуре), обуку и контроле [265]. **Управљање безбедносним ризиком** укључује идентификацију опасности, анализу ризика и контролу ризика. При томе, ефикасан систем управљања ризиком сарађује и интерно (унутар организације) и екстерно (унутар индустрије) и третира управљање ризиком као нестатичан, итеративни процес. Управљање безбедносним ризиком и **осигурање безбедности** уско су повезани – процес управљања безбедносним ризиком омогућава успешно остваривање безбедности, јер захтева дефинисање процеса и очекивања, као и управљање ризиком на прихватљивом нивоу. Унапређење безбедности може се описати као процес одозго-надоле, тј. процес који почиње од извршног руководства и који се спушта до појединачних запослених кроз безбедносну политику. Међутим, **промоција безбедности** не почиње и не завршава се само унутар организације; радне групе за регулисање и сарадњу имају улогу да дефинишу и подстичу најбољу праксу управљања безбедношћу [265].

Процена ризика по **сајбер безбедност** је континуирани аналитички и систематски процес процене нивоа ризика, која се постиже идентификацијом потенцијалних сајбер претњи, а које имају негативан утицај на ваздухопловне системе и потенцијални утицај на авио-операције, инфраструктуру и др. Квалитативна и квантитативна **методологија** за процену ризика, укратко, састоји се од:

- идентификације величине система који треба заштитити – потенцијалне претње се идентификују разумевањем функционисања различитих система навигације (комуникација, навигација, надзор и умрежавање), затим, дефинисањем компоненти система, радног окружења, међусобних односа с трећим лицима, као и описом различитих система ваздушне навигације

[122] У ваздухопловству, формално управљање безбедносним питањима је сада ICAO стандард, и имплементација *Security Management Systems* (SeMSs) представља најбољу праксу. Иако SeMS и SMS имају сличне принципе и заснивају се на упоредивим процесима, неопходно је побољшати/олакшати кооперативни паралелни рад ова два менаџмента [263].

- идентификације потенцијалних сценарија сајбер напада, који би могли нанети директну/индиректну штету ваздухопловном систему (претње које могу утицати на интегритет, поверљивост и доступност различитих услуга ваздушне навигације)
- одређивања вероватноће напада на основу различитих фактора укључујући способности и намере нападача, без разматрања тренутних безбедносних мера (дефинисање одређених фактора за процену вероватноће претњи, као што је потребно знање или стручност, историјски подаци о настанку претњи, као и цена и доступност алата који се користе за извођење напада)
- одређивања утицаја најгорег сценарија претње у ваздухопловној безбедности, ефикасности/ефективности, економској/финансијској, политичкој и репутацији/јавном поверењу, што зависе од природе и обима последице сајбер-напада
- процене нивоа ризика на основу резултата тестова вероватноће, процене рањивости, као и утицаја претњи, у циљу добијања свеобухватне слике ризика за потенцијалне нападе на системе ваздушне навигације.

За добијање нумеричке вредности нивоа ризика различитих ваздухопловних система од специфичних претњи, користи се ICAO методологија процене безбедносног ризика [266]. Као што је детаљно објашњено у раду [149], пратећи ICAO методологију, формира се матрица за процену ризика сигурности и безбедности, која рангира нумеричке вредности нивоа ризика у три различите категорије: прихватљиво (нису потребне додатне мере за ублажавање и контролу ризика), подношљиво (може се толерисати на основу додатних мера за смањење ризика) и недопустиво. На тај начин, могу се графички приказати и сагледати процењени безбедносни ризици по различите комуникационе протоколе (VHF гласовна комуникација, CPDLC и ACARS), затим, навигационе системе (GNSS, ILS и VOR), као и системе надзора (PSR, SSR, MLAT[123] и ADS–B).

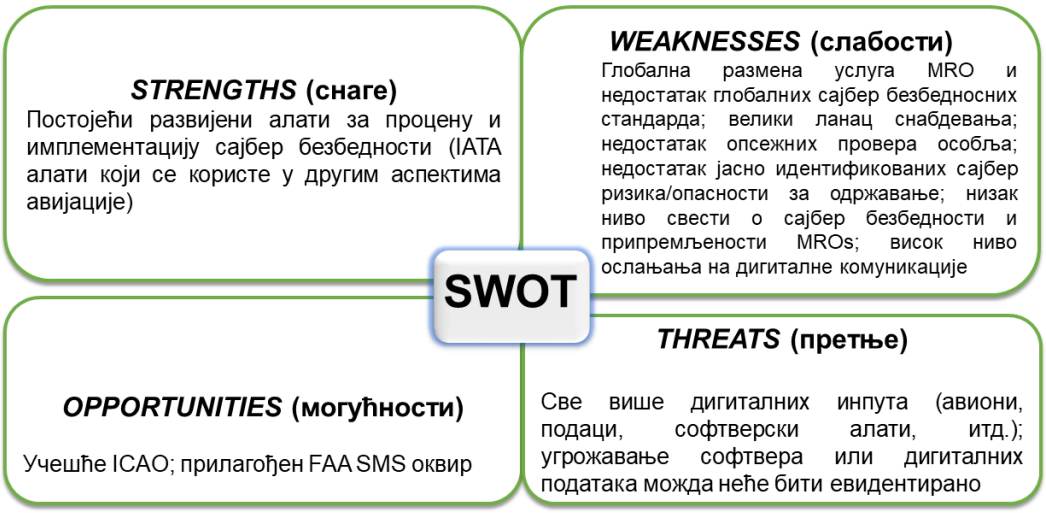
Према DHS-у, кључне ризичне области у ваздухопловству су: системи глобалног позиционирања, операције и IT инфраструктура, ATC, бежичне мреже, одржавање и "друге непознате претње" [188]. На пример, у ваздухопловству, индустрија *maintenance, repair* и *overhaul* (**MRO**), тј. индустрија одржавања, поправке и ремонта, показује нарочите слабости у вези са сајбер безбедношћу, а рањивости високог нивоа односе се на софтвер и дигиталне податке.

Користан алат за идентификацију и категоризацију аспеката унутрашњег и спољашњег окружења, јесте SWOT (*strengths, weaknesses, opportunities, threats*)

[123] MLAT (*multilateration*) је независна технологија надзора, који се заснива на принципу *time difference of arrival* (TDoA) [267, 268]. За разлику од зависних техника надзора као што је ADS–B, MLAT је независан систем, код кога се позиција авиона математички израчунава решавањем TDoA скупа једначина. Стога, чак и ако постоји измена у садржају поруке у MLAT систему између транспондера у авиону и сензора на земљи, локација авиона се одређује коришћењем времена потребног за пријем порука, а не на основу садржаја поруке, што значајно повећава безбедност. Међутим, MLAT пријемници на земљи морају бити синхронизовани с GPS, који је подложан нападима ометања (*jamming*) и лажирања (*spoofing*), тако деградирајући тачност локализације авиона добијеног помоћу MLAT-а.

анализа, тј. анализа снаге, слабости, могућности и претњи. На пример, окружење може бити, у оквиру ваздухопловства, поменута MRO индустрија (сл. 13) [269].

С друге стране, техничка процена безбедности, подразумева или процену угрожености, или тестирање "продора". Иако су обе категорије део исте технике, постоје значајне разлике у начину њиховог извођења, као и утицају који имају на системе–мете [137]. **Процена угрожености** представља евалуацију техничких пропуста у систему. Најчешће се изводи као тзв. *white-box* тестирање,[124] које подразумева документовање безбедносних слабости/проблема, од стране лица која спроводе тестирање (најчешће програмери), а који током процене угрожености, имају приступ документацији, конфигурацији, као и особљу, у циљу потпуног сагледавања безбедносне ситуације, тј. свих потенцијалних безбедностих слабости/проблема. С друге стране, **тестирање "продора"** подразумева укључивање покушаја искоришћења слабости у циљу утврђивања озбиљности и процене изводљивости сајбер напада.



Слика 13. MRO (*Maintenance*, *Repair* и *Overhaul*) индустрија – SWOT анализа (модификовано и преузето из [269])

На пример, **SCADA** (фуснота 63, део 3.1.2.) преферира процену угрожености, јер омогућава свеобухватнију анализу безбедносног стања [137] У овом случају, процене угрожености односе се на:

- усклађивање захтева – одређивање испуњености захтева; SCADA системи морају бити у складу с *North American Electric Reliability Corporation Critical Infrastructure Protection*, тако да је неопходно обезбедити ефикасан SCADA

[124] *White-box* тест јесте метода тестирања софтвера и добила је такав назив, јер софтверски програм, који анализира програмер, изгледа као бела, транспарентна кутија у којој се све јасно сагледава. У овој методи, дакле, унутрашња структура/дизајн софтвера позната је ономе ко врши тестирање, тј. програмеру, који бира инпуте (за налажење путева кроз кôд) и детерминише излазе. На пример, програмер анализира кôд имплементације одређене области на *web* страници, детерминише све легалне (валидне и невалидне) и нелегалне уласке, као и верификује резултате у односу на очекиване.

методолошки тест (способан да процени сваки појединачни захтев за сајбер безбедност)

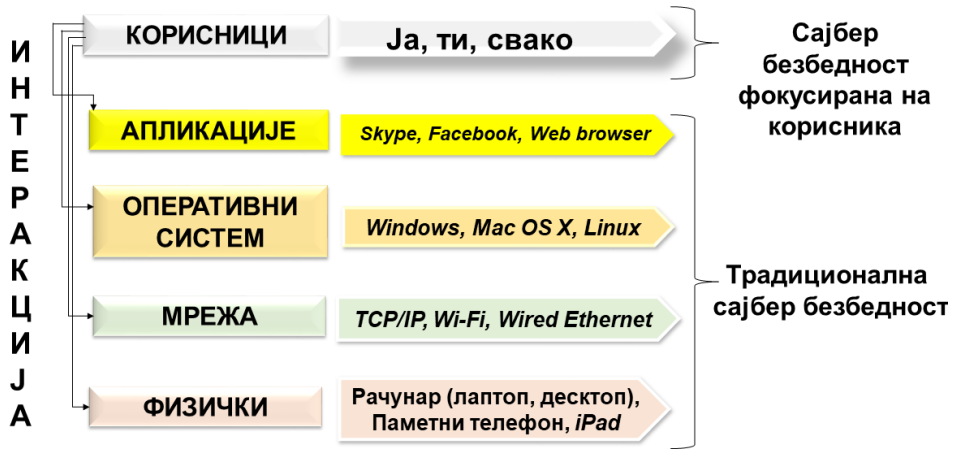
- преглед мрежног саобраћаја – за потпуно разумевање мрежне комуникације (којим мрежним услугама се приступа и који/какви подаци циркулишу преко мреже)
- разматрање конфигурације система – зависи од познавања врсте безбедносних питања у оквиру софтвера и тренутне добре праксе (за већину широко коришћених IT софтверских производа на располагању су документоване безбедносне смернице, за већину SCADA софтвера није рађена таква врста анализе)
- *Network Discovery, Port* и *Protocol Identification* – администратор има информације о "домаћину" и комуникационим протоколима; међутим, за валидацију било каквих претпоставки, неопходан је *network discovery* процес (омогућава повезивање и међусобно комуницирање мрежних уређаја преко лакалне мреже)
- скенирање рањивости – процена сајбер рањивости, коју су развиле US *Computer Emergency Readiness Team* (US-CERT) и *National Institute of Standards and Tecnology* (NIST), и идентификује следеће кључне слабости: бежичне и мрежне приступне тачке, незаштићене *Structured Query Language* базе података, неадекватно конфигурисани *firewalls* (рачунарски систем, тј. филтер између персоналног рачунара и спољашњег "света", који кроз свој "филтер" пропушта само оне податке, а који су у складу с постављеним правилима заштите), итд.

Сајбер безбедност SCADA система на аеродромима захтевају високе сајбер безбедносне стандарде/мере и рутинске провере сајбер рањивости. Евалуација актуелног стања указују на потенцијалне рањивости у областима у којима су неопходна додатна истраживања. Недостаци у проценама безбедности, узроковане разликама између IT и SCADA, односе се на ослањање на мрежне протоколе, недокументоване верзије софтвера, као и адекватних конфигурација, и одговорност за очување стабилности система током процеса процене.

Информациона безбедност (део 2.2.1.), најчешће означава конфликт између хакера и професионалца из области сајбер безбедности. Појам информациона безбедност користи се као свеобухватни термин, који дефинише сва питања безбедности, а који су у вези с технологијом, или се користи као суб-класификација шире категорије, као што је информациона сигурност. Без обзира на то, **безбедност/сигурност** је процес заштите информација од претњи. Може се објаснити и тзв. C–I–A моделом: **C** (*Confidentiality,* поверљиво) – спречити неовлашћене кориснике да читају/имају приступ информацијама, **I** (*Integrity,* интегритет) – осигурати да неовлашћени корисник не мења информације и **A** (*Availability,* доступност) – омогућити приступ (према потреби) овлашћеним корисницима.

IT безбедносна процена најчешће се фокусира на контролу безбедности и механизама у апликацијама, оперативном систему, мрежи или физичко-технолошким слојевима (сл. 21). Међутим, због експанзије коришћења BYOD на аеродромима, као што је претходно поменуто, неопходно је постојање адекватног материјала у вези са сајбер безбедношћу и едукација и обука свих запослених на

аеродромима, као и едукација корисника аеродрома (јавности). Иако су основе рачунарске безбедности техничке природе, бројни безбедносни концепти су емпиријски, и могу бити, уколико су адекватни,[125] веома корисни и онима с минималним техничким знањем, а који се свакодневно конектују на интернет или *wireless* мрежу, "сурфују", размењују информације преко друштвених мрежа, итд. Свака од ових активности је потенцијално ризична и може имати штетне последице, којих корисник, у већини случајева, није свестан.



Слика 14. Различити слојеви сајбер безбедности на аеродромима у доба експанзије BYOD-а (модификовано и преузето из [137])

На аеродромима, и поред свих техничких достигнућа, не постоји потпуна заштита IT система од свих сајбер претњи. Свакако, у остваривању безбедних аеродромских мрежа, неопходно је избалансирати потебе и оперативну функционалност, у циљу неометаног функционисања аеродрома, тј. обезбеђивање одвијање критичних операција аеродрома без ометања аеродромских операција.

[125] За припрему приручника/мултимедијалних материјала за едукацију у вези са сајбер безбедношћу, корисника/запослених на аеродромима, неопходно је обратити пажњу на следеће чињенице [270]: за остваривање безбедности, неопходни су значајни финансијски ресурси, као и време (уколико је информација/објекат, коју треба заштити мале вредности, нема смисла трошити ресурсе за њихову заштиту; безбедност се остварује кроз вишеслојну одбрану (не постоји јединствен сигурносни механизам, који обезбеђује апсолутну заштиту свих информација од потенцијалног напада, тако да слојевити приступ отежава хакерски напад, с обзиром на то да "уљез" мора заобићи већи број безбедносних механизама за добијања приступа информацијама); апсолутна безбедност не постоји (у свету рачунара, ни један сигурносни систем не може бити савршен).

5. GPS/GNSS: ФУНДАМЕНТАЛНИ КОНЦЕПТ И САЈБЕР БЕЗБЕДНОСТ

> *"С настављањем продирања GPS-а у цивилну инфраструктуру, GPS постаје примамљива мета коју могу искористити (малициозни) појединци, групе или државе...Потенцијал за ометање постоји. Постоји могућност да се GPS пријемник подстакне да продукује погрешне информације."* [271]

Global Positioning System (GPS) је свемирски радио-навигациони систем (сателитска навигација), tj. констелација сателита, који емитују радио-фреквентне (RF) таласе у циљу одређивања прецизне локације на/у близини површине Земље. Овај систем је најпре (50.-их година 20. века), развијен и коришћен искључиво у војне сврсхе. Касније, од 80.-их година 20. века, GPS је стављен на располагање и за широку, цивилну употребу, а с обзиром на значајан потенцијал у различитим областима примене.

Постоји неколико система сателитске навигације којима управља и које одобрава ICAO, и то су GPS (USA), GLONASS (Русија), Galileo (Европа), BEIDOW (Кина), итд. Стога, GNSS (*Global Navigation Satellite System*) је заједнички термин за различите врсте навигационе инфраструктуре/система, који, захваљујући побољшаном нивоу тачности и одсуству ограничења која намећу застарела радио-навигациона средства, може глобално искористи све предности навигације засноване на перформансама. GPS и GLONASS системи су потпуно оперативни, док европски Galileo, који је започео испоруку својих услуга у децембру 2016. године, тренутно располаже са 26 сателита на небу (од јула 2019.), од којих су 22 у потпуности оперативна. Кинески BeiDou има 25 сателита на небу (од августа 2018.), од којих су 23 оперативна [228]. Према ICAO (Анекс 10) [272], тренутно су одобрени GPS L1 и GLONASS G1 фреквенцијски опсези за ваздухопловство, ако се у будућности очекује и коришћење фреквенцијских опгега GPS L5 и Galileo E1/E5a (део 5.1.1).

Сигнали GNSS-а, користе се у различитим областима примене на Земљи, за добијање информација о позицији, навигацији и времену (*position, navigation* и *time*, PNT), а с модернизацијом GPS-а, GLONASS-а и BEIDOW-а, као и додатних регионалних сателитских система (нпр. јапански QZSS и индијски NavIC), испитују се могућности коришћења мулти-констелационог GNSS-а у свемиру [273]. Употреба мулти-констелације, која се састоји из више од 100 активних GNSS сателита, обезбедиће пораст покривености сигналом и различитост коришћених система, што ће побољшати укупне PNT перформансе и отпорност система, како на Земљи, тако и у свемиру [274, 275]. Такође, Јужна Кореја планира свој сателитски навигациони систем (*Korean Positioning System*), за пружање услуга регионалног навигационог система преко Корејског полуострва [276, 277]. Истраживањима у вези с развојем ових инфраструктурних система и коришћењу GNSS технологије у свемиру, баве се NASA [278], *European Space Agency* (ESA) [279], и други пројекти [280].

У ваздухопловству, радио-навигациона средства неопходна су за одређивање позиције авиона и навођење у различитим фазама лета, као што су полетање,

слетање и крстарење (*landing, approach* и *en-route*) и главне су компоненте АТС-а, заједно са системом за комуникацију и надзор [281]. Међутим, системи који се ослањају на сателитске технике навигације, као што је GPS/GNSS или ADS–B (глава 6), због веома једноставног безбедносног протокала, који не обезбеђује потпуну аутентификацију и енкрипцију, рањиви су на различите врсте сајбер напада. У цивилном ваздухопловству и АТС-у, иако GNSS технологија није једино навигационо средство[126], улога и примена ове технологије је у константном порасту, како у генералној авијацији, тако и код употребе UAS, тј. дронова (фуснота 106, поглавље 4), за чије управљање су неопходне PNT информације, које се добијају од GNSS-а.

Због свега тога, у делу 5.1, описан је фундаментални концепт GPS/GNSS технологије, у обиму који је неопходан за разумевање релевантних питања у вези са сајбер безбедношћу GNSS-а (поглавље 5.2), тј. безбедносних рањивости и сагледавање различитих врста сајбер напада на GNSS (део 5.2.1), као и примену различитих методологије за процену сајбер-безбедносних ризика GNSS-а (део 5.2.2). Најновији правци у анализи GPS података базирају се на фази логици и вештачкој интелигенцији, тако да је у поглављу 5.3. дат кратак опис концепције фази логике (основни појмови, анализа и методе фази система закључивања), као и нових фази алгоритама за класификовања података и примена у области авијације.

5.1. GPS/GNSS ТЕХНОЛОГИЈА

GPS/GNSS системи омогућавају одређивање положаја авиона, као и дају друге информације, на основу емитованих сателитских сигнала [282]. На основу ових сигнала, примљених с најмање четири сателита, GNSS пријемници (у авиону), процењују тродимензионалну (3D) позицију авиона (део 5.1.1) у глобално стандардизованом координатном систему (WGS-84). За разлику од навигационих система, која користе конвенционална земаљска радио-навигациона средства и која имају бројна ограничења (нпр. финансијски трошкови инсталирања и периодични захтеви за инспекцију) [283], употреба GNSS-а омогућава непрекидно ажурирање позиције авиона, што омогућава да авион прати жељени план лета, без ограничења које намеће нпр. орографија, а која спречава пријем сигнала земаљских радио-навигационих средстава.

Иако је GPS једини потпуно оперативан GNSS ″прве генерације″, као што је претходно поменуто, доступан је и руски Глобални навигациони сателитски систем, GLONASS (обухвата Русију и суседне државе), док Европа развија GNSS ″друге генерације″, под називом *Galileo* програм, а који је потписала и Кина (2003). GNSS је сада допуњен с неколико додатних сателитских система, генерички названих S*pace Based Augmentation Systems* (SBAS) [149] јер емитују додатне

[126] За навигацију, у употреби су и други навигациони системи, који користе конвенционална земаљска радио-навигациона средства, као што су ILS, DME и VOR (поглавље 3.1).

сигнале, које пријемник може декодирати и користити (заједно са глобалним GNSS сигналима) у сврху побољшања перформанси позиционирања[127].

SBAS[128] је регионални сателитски систем, у коме корисник (нпр. авион) прима информације са сателита. Користи мрежу земаљских референтних станица за праћење сателитских сигнала; централне станице обрађују податке примљене од земаљских референтних станица, и генеришу SBAS појачане сигнале, а *uplink* станице шаљу поруке гео-стационарним сателитима, а које се могу слати авионима.

Поред SBAS-а, постоји и *Ground-Based Augmentation System* (**GBAS**), диференцијални навигациони систем који помоћу GNSS пријемника (постављених на познатим и претходно испитаним локацијама), врши процену и мониторинг диференцијалних корекција у реалном времену с примљеним GPS сигналима, као што су грешке сателита и јоносфере. Ове диференцијалне корекције преносе се, путем *Ground-Based VHF Data Broadcast* (VDB) до авиона у близини аеродрома. GBAS је алтернатива за скупе ILS системе, с додатном предношћу, што може заменити више ILS распоређених на више аеродромских писта; међутим, у односу на SBAS, који је регионални сателитски систем, GBAS појачава GPS сигнале у близини аеродрома и емитује их путем VDB-а.

GNSS систем за појачање сигнала јесте и *Aircraft-Based Augmentation System* (**ABAS**), који допуњава и/или интегрише информације добијене од GNSS пријемника с другим навигационим информацијама доступним у авиону. Постоје два типа ABAS-а: *Receiver Autonomous Integrity Monitoring* (RAIM)[129], који користи искључиво GNSS информације, и *Aircraft Autonomous Integrity Monitoring* (AAIM), који користи *on-board* сензоре, као нпр. барометарски висиномер или *Inertial Reference System* (IRS) [284]. У поређењу са SBAS-ом и GBAS-ом, главна предност ABAS-а је његова исплативост – побољшање услуге, без финансијских трошкова за додатну инфраструктуру [284].

GPS се састоји из три сегмента (сл. 15), и то су:

- свемирски
- контролни[130]

---

[127] За потребе летења на рути, стандрадни GPS систем је задовољавајуће прецизности. Међутим, за фазе лета, као што су прецизни прилаз и слетање, GPS систем није задовољавајуће прецизности За повећање тачности навигације, предложено је појачање GNSS сигнала, нпр. коришћењем SBAS-а.

[128] Постоје четири оперативна SBAS система, признатих од стране ICAO, и то су: *Wide Area Augmentation System* (WAAS) у Северној Америци, *European Geostationary Navigation Overlay Service* (EGNOS) у Европи, *GPS-Aided GEO Augmented Navigation* (GAGAN) у Индији и *Multi-functional satellite augmentation system* (MSAS) у Јапану [149].

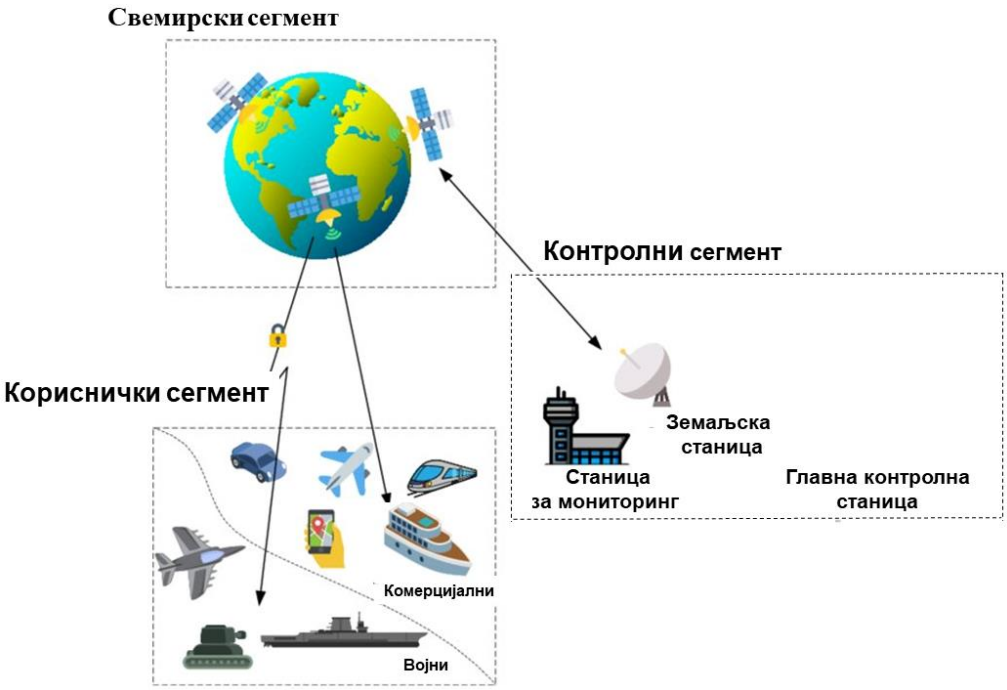
[129] RAIM је најчешће коришћен систем за мониторинг интегритета; то је алгоритам у пријемнику, који је омогућен уколико постоји најмање пет сателита одговарајућег геометријског распореда (у констелацији).

[130] Контролни сегмент GNSS-а, тј. контролни центар (састоји се из пет земаљских станица, од којих је главни контролни пункт војна база *Schriever* у Колораду, USA), проверава стање, позицију, брзину и висину сателита, а до мањих одступања у мереним величинама, може доћи услед нпр. гравитације Земље или радијације, што се узима у обзир при прецизном одређивању положаја. Ажурирање прецизне путање сателита, врши се у просеку свака 4 h и подаци о ажурираним орбитама, шаљу се сателитима преко земаљских радио антена.

- кориснички.

Свемирски сегмент GPS-а сачињава 27 сателита (констелација), од којих су 24 навигациона и 3 су резервна. GPS сателити називају се NAVSTAR (*Navigation Satelite Timing and Ranging*), а то је и службени назив USA министарсва одбране за GPS. Сваки сателит обиђе Земљу за 12 h, као и понавља исту путању и конфигурацију изнад одређене тачке, једном у приближно 24 h. Постоји 6 орбиталних равни (са 4 сателита у свакој равни), које су међусобно под углом од 60°, као и под углом од 55° у односу на екваторијалну раван. GPS систем има 3 фреквентна опсега, L1, L2 и L5 (L5 су L2 и још увек су у фази развоја [285]).

Дакле, све врсте GNSS сателита емитују на најмање два фреквенцијска опсега: на фреквенцији L1 – криптовани војни кôд, тзв. P(Y) и нешифровани цивилни кôд (C/A), као и на фреквенцији L2 (понављање P(Y) кôда). Сви сателити емитују сигнале на две фреквенције, и то: 1575,42 MHz и 1227,6 MHz. У табели 4 дате су сумарно карактеристике GNSS, као и навигационих система који користе конвенционална земаљска радио-навигациона средства (ILS, VOR и DME), док ће детаљи оперативног концепта и GNSS сигнала бити дати у делу 5.1.1.1.



Слика 15. Архитектура GPS-а (модификовано и преузето из [228])

За већу тачност навигације (фуснота 127), предлаже се коришћење различити системи за појачање, као што је систем појачања заснован на авиону (ABAS), земаљски систем (GBAS), као и сателитски систем (SBAS) појачања.

Табела 4. Врсте радио-навигационих средстава (употреба, врста и опсег фреквенција) [149]

Навигациони систем	Употреба	Врста	Фреквенција/Опсег фреквенције
GNSS	Одређивање 3D позиције и времена	Сателитско	L1: 1575,42 MHz L2 1227,6 MHz
ILS	*Localizer*; навођење прилаза по правцу, тј. одређивање курса навођења до средишње линије полетно-слетне стазе Прилазна раван *(glide slope)*: даје информације пилоту о вертикалне девијације авиона од угла прилаза полетно-слетној стази	Земаљско	*Localizer*: 108–111,975 MHz Прилазна раван: 328,6–335,4 MHz
VOR	Одређивање *bearing* угла*	Земаљско	108–117,975 MHz
DME	Одређује косу удаљеност између авиона и земаљског радио-навигационог средства	Земаљско	962–1213 MHz

**bearing* угао – угао између правца кретања авиона и правца север-југ

5.1.1. GPS/GNSS – фундаментални концепт

GPS архитектуру (сл. 15), као што је претходно поменуто, сачињавају три сегмента, и то [228, 285–287]:

- Свемирски сегмент (сачињавају га сви сателити у констелацији) – сазвежје сачињава 24 сателита, која се састоји од 6 скоро кружних орбита, које су под углом од 55° у односу на екваторијалну раван на алтитуди од 20.183 km. Сваки сателит обиђе Земљу, тј. направи круг око планете, за 11 h 57 min 58 s. Тако, у видној линији на било којој позицији на планети, увек се налазе 4 сателита, што омогућава одређивање локације (при нормалним атмосферским условима). Основне функције свемитског сегмента су да емитује GNSS сигнале, прими корекције орбита од земаљског сегмента и примени их.
- Земаљски сегмент, који је одговоран за функционисање станица за праћење, контролу и ажурирање – основне функције овог сегмента су: надгледање сателита, дефинисање орбита за сваки сателит у циљу предикције ефемерида и података из алманаха и одређивање висине и локације сваког сателита, као и слање корекција сателитима, на начин да задрже адекватне орбите.
- Кориснички сегмент (састоји се од свих врста пријемника GPS сигнала) – садржи широк спектар пријемника (војни, пријемници за цивилну употребу,

итд.). Основне фунције овог сегмента су да: прима сигнале GNSS система и процењује њихов статус; изврши мерење времена пропагације сигнала; изрши мерења узимајући у обзир Доплеров ефекат; израчуна локацију пријемника; израчунава брзину корисника и омогући мерења времена.

Дизајн свих GNSS система (GPS, GLONASS, Galileo, BeiDou, итд.), тј. система сателита (констелација) веома је сличан, и сваки омогућава преношење три основне поруке, и то су [288]:

- сигнал домета за позицију, брзину и време (PVT)
- прецизни подаци о ефемеридама, који одређују тачан положај сваког појединачног сателита
- алманах, који одређује положај и орбите свих сателита у констелацији (сазвежђу), заједно с информацијама о статусу изабраног сателита за праћење.

Основни степен интероперабилности омогућава GNSS пријемницима да примају сигнале добијене од четири главна сателитска сазвежђа, без замрачење у областима лошег пријема, а с обзиром на сателите из других сазвежђа који су видљиви. Процењује се да ће око 120 сателита бити доступно, када сви поменути GNSS системи буду у потпуности распоређени, с 30–40 видљивих (оперативних) сателита у сваком тренутку [289, 290]. Све врсте GNSS сателита емитују сигнале на неколико L спектралних трака, тј. фреквенцијска опсега, од 1 GHz до око 1,6 GHz, које се означавају са L1, L2, G1, G2, итд. При томе, L1 на фреквенцији 1575,42 MHz обухвата криптовани војни кôд, тзв. P(Y) и нешифровани цивилни кôд (C/A), док L2 на фрекценцији 1227,6 MHz је понављање кôда P(Y).

Дизајн GNSS-а омогућава добијање три основна параметра, и то су: удаљеност, време, као и географска ширина, дужина и висина. GPS (сл. 16), користи сателите, тј. сателитске предајнике S_i (i = 1–4), чије су локације L_i^S (koordinate, x_i^S, y_i^S i z_i^S) познате [291]. Сваки предајник опремљен је веома прецизним синхронизованим сатом за мерење тачног системског времена, t^S и емитује навигациони сигнал $s_i(t)$, (*low auto-/cross-correlation*), који садржи временске ознаке и одступања сателита од предвиђене трајекторије. Сигнал се преноси брзином c.

Пријемник (V), чији 3D положај одређују координате (L), омнидирекционалном антеном прима комбиновани сигнал, g (L,t) од свих сателита, у опсегу, датом изразом:

$$g(L,t) = \sum_i A_i\, s_i \left(t - \frac{|L_i^S - L|}{c}\right) + n(L,t) \tag{1}$$

где је: A_i слабљење сигнала на путу од L_i^S до L; $|L_i^S - L|$ је Еуклидска разлика између L_i^S и L; $n(L,t)$ је шум.

Захваљујући карактеристикама навигационог сигнала, $s_i(t)$, могу се раздвојити сабирци у изразу (1) и тако добити релативна фаза кôда, ID сателита и садржај поруке користећи реплику кôда. На основу ових података и релативне фазе кашњења, пријемник идентификује временско кашњење, $\frac{|L_i^S - L|}{c}$, за сваки сателит, односно "опсеге": $d_i = L_i^S - L$, одакле се може, уколико је позната позиција предајника, L_i^S, добити 3D положај, L пријемника. Како је часовник пријемника у

кашњењу, тј.има временски помак, δ у односу на егзактно системско време, t^S, тако да пријемник даје "псеудо-опсеге":

$$R_i = d_i - c \times \delta = d_i - \Delta \quad (2)$$

Познавајући растојање од сваког сателита (најмање четири) и решавањем система нелинеарних једначина (2) по L и δ, добијају се прецизни положаји и времена, који се користе за навигацију, позиционирање и тачну расподелу времена.

Како је $L_i^S = (x_i^S, y_i^S, z_i^S)$ и $L = (x,y,z)$, једначина (2) може се трансформисати у израз:

$$\left(x - x_i^S\right)^2 + \left(y - y_i^S\right)^2 + \left(z - z_i^S\right)^2 = (R_i - \Delta)^2 \quad (3)$$

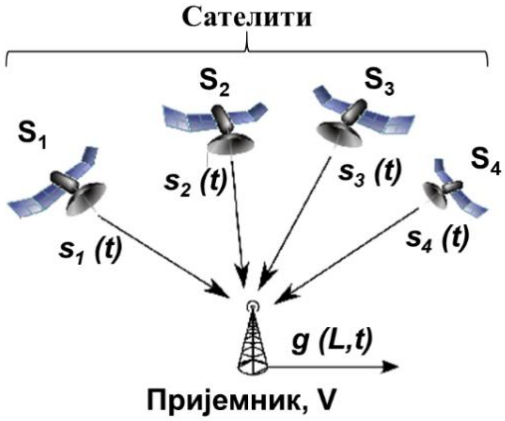
Геометријски, једначине (3) представљају хиперболоиде, чији пресек, тј. решење система једначина, одређује положај пријемника (сл. 17) [288]. Систем једначина (3) решава се нумеричким методама, као нпр. Њутновом методом [292].

GNSS је оригинално дизајниран за пренос сигнала са велике удаљености у правцу центра Земље (геоцентричном правцу), тако да код коришћења концепта *space service volume* (SSV)[131], и када је пријемник GNSS сигнала на позицији већој од 3.000 km са супротне стране Земље, сигнали би требало би да буду примљени и у *nadir*[132], као и у правцу зенита. Међутим, на растојањима већим од 20.000 km, само антена лоцирана у правцу *nadir*-а може примити GNSS сигнале [293]. У овој ситуацији, долази до погоршања перформанси навигације, тј. појављује се ефекат сенке генерисаних сигнала, јер није задовољен минимални број видљивих сателита (четири), неопходних за једно позиционирање GNSS-а. Поред тога, услед велике удаљености путање, тј. губитка слободног простора, снага примљених GNSS је мала. За побољшање перформанси GNSS сигнала, коришћење интероперабилних GNSS система је у предности у односу на коришћење једног GNSS система, у погледу видљивости сателита, примљене снаге сигнала, трошкова, као и заштите животне средине [274, 277, 294, 295].

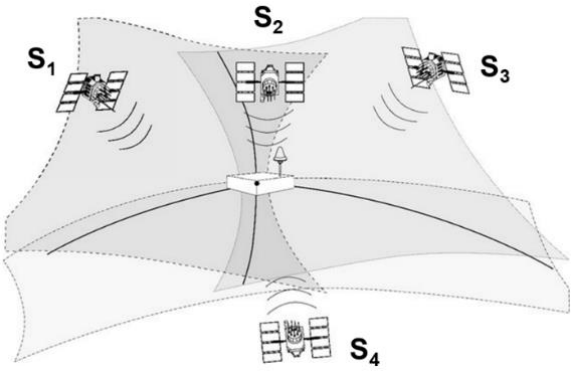
---

[131] С порастом растојања простирања сигнала, тј. смањењем слободног простора, долази до смањења јачине GNSS сигнала. Због тога је неопходно одредити минималну снагу примљених сигнала, да би се GNSS сигнали користили на геостационарној орбити (GEO). Тако, NASA је дефинисала концепт *space service volume* (SSV), базираног на карактеристикама GNSS сигнала на различитим висинама – део од површине Земље до 3.000 km (*terrestrial service volume*, TSV), и део од 3000 km до 36.000 km (SSV). На пример, *Low-Earth Orbit*, LEO (< 3000 km) у TSV, има скоро константну јачину сигнала, а PNT се може проценити користећи само GPS, без прекида сигнала. GPS пријемници, који се користе на Земљи, могу се користити и од сателита у TSV-у уз незнатне модификације (корекција за Доплеров ефекат). SSV се класификује као *Medium Earth Orbit* (MEO) SSV и *High Earth Orbit* (HEO)/*Geostationary Earth Orbit* (GEO) SSV на основу алтитуде од 8000 km. У MEO SSV, могу се примити GPS сигнали са више од четири сателита и постићи прецизност од 1 m. У HEO/GEO SSV, сигнали се преносе са супротне стране од Земље и долази до прекида GPS сигнала. Штавише, јачина сигнала у NEO/GEO SSV је мања од оне код нижа од оне код TSV и MEO SSV, али је тачност положаја у оквиру 100 m [273].

[132] *Nadir* представља правац испод одређене локације, супротно од правца Зенита.

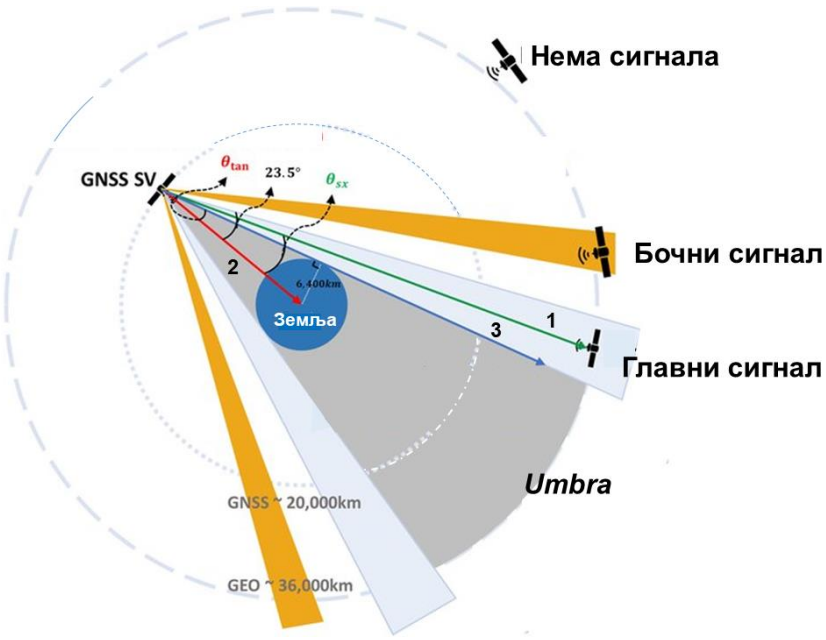


Слика 16. GPS пријемник (*V*) користи навигационе сигнале $s_i(t)$ (i = 1–4) сателита (S_i, i = 1–4) за одређивање 3D положаја (*L*) и временског помака (δ) GPS пријемника (модификовано и преузето из [291])



Слика 17. Позиција пријемника добијена решавањем система нелинеарних једначина (3) (модификовано и преузето из [288]

Орбита GNSS сателита је на висини од 20.000 km. GNSS сателити круже око Земље и преносе сигнале у правцу центра Земље. Коришћење сигнала, који се преносе са супротне стране Земље у SSV, захтева посебну геометрију GNSS-а. Антена у положају *nadira*, прима сигнал за одређену вредност тангенцијалног угла од GNSS SSV до центра Земље ($\theta_{\tan}$) и угла између вектора 2 (вектор од GNSS сателита до пријемника) и вектора 3 (правац тангенте GNSS сателита на вертикалу Земљине површине, θ_{sx}). Уколико се нпр. претпостави да је полуширина бочног таласног фронта 27–39°, област у којој се добија сатитска видљивост θ_{sx}, је: $\theta_{tan} < \theta_{sx} < 23{,}5° <$ ширина главног таласног фронта, за $27° < \theta_{sx} < 39°$ (ширина бочног таласног фронта) [295]. Геометријска структура GNSS сигнала, који се примају на геостационарним орбитама (GEO), дата је на сл. 18.



Слика 18. Геометрија GNSS сигнала у гео-синхронизованој земаљској орбити (GEO) (модификовано и преузето из [295]
1 – вектор (растојање од GNSS сателита до пријемника); 2 – вектор (растојање од GNSS сателита до центра Земље); 3 – правац тангенте GNSS сателита на вертикалу Земљине површине; *Umbra* – тамна, унутрашња сенка Земље, кружног попречног пресека

У оваквим и сличним истраживањима, нумеричим симулацијама, анализирају се различита сценарија конфигурације и доступности GNSS сигнала. Показано је да комбинација сигнала (главног и бочног) и компатибилност више констелација, може повећати број видљивих сателита, побољшати конфигурацију геометрије, смањити *Geometric Dilution of Precision* (GDOP)[133] и тако побољшати доступност GNSS сигнала, тј. остварити задовољавајуће перформансе навигације за SSV пријемнике [274, 294–297, 277].

GNSS пријемници су данас веома доступни, јефтини и компактни уређаји, и широко се користе у различитим системима (нпр. системи за надзор и прикупљање података, SCADA (фуснота 63), у мобилним телефонима и бројним широко коришћеним производима. GNSS је атрактиван, јер даје прецизну локацију пријемника [286] и времена [298] с тачношћу ± 4 m и ± 10 ns, редом.

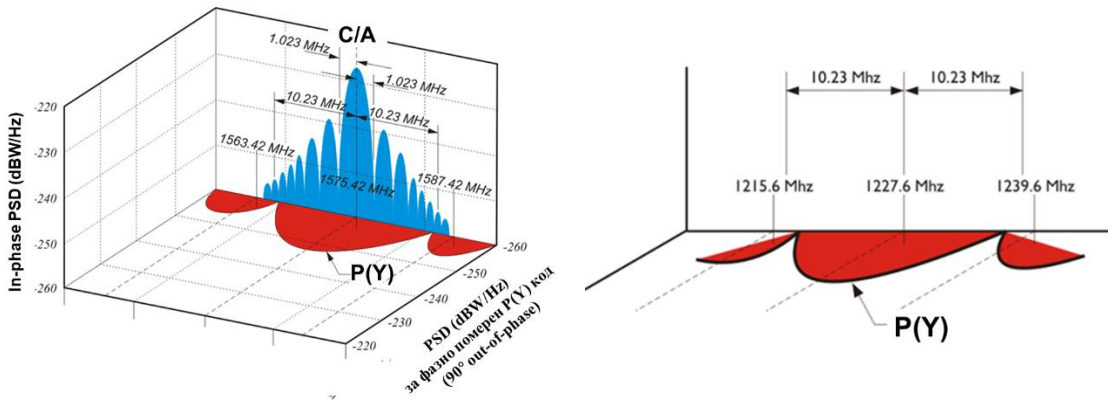
[133] GDOP је индикатор квалитатета геометрије сателитске констелације, тј. утицаја геометрије сателита на тачност GPS сигнала, и грубо речено, представља однос грешке одређивања положаја и грешке домета. Мање вредности GDOP-а, указују на већу тачност одређивања GPS положаја, и обрнуто. GDOP се добија математичким поступком базираном на геометријским односима између положаја пријемника и положаја сателита који се користе за навигацију.

5.1.1.1. GPS сигнали

Сви типови GNSS система сателита, као што је поменуто, емитују сигнале на најмање два опсега, и то: L1 сигнал на фреквенцији 1575,74 MHz, који обухвата шифровани прецизни војни кôд, означен са P(Y) (могу му приступити само овлашћени корисници) и груби/аквизициони, нешифровани цивилни кôд (C/A), док се на фреквенцији 1227,6 MHz (сигнал L2), кôд P(Y) понавља. L1 сигнал користи се у SBAS-у (поглавље 5.1) који се примењује у цивилном ваздухопловству; GPS сигнали се појачавају сигналима са гео-стционарних сателита користећи L1 кôд.

График зависности спектралне густине снаге (снага сигнала у dBW по пропусном опсегу у Hz) сигнала L1 и L2 у функцији фреквенције, дати су на слици 19 (а и б). Проширени спектар C/A цивилног кôда на носачу L1, има главну траку на 1575,74 MHz и споредне траке са обе стране централне траке, тако да је спектар проширен за око 20,46 MHz. У односу на C/A кôд, P(Y) кôд је фазно померен за 90° и има централну (главну) траку на 1227,6 MHz. График зависности спектралне густине сигнала L2 (сл. 19 б), сличан је оном за L1, осим што нема C/A кôд, с обзиром на то да се он не преноси на L2 фреквенцији.

(а) (б)



Слика 19. Дијаграм спектралне густине снаге сигнала L1 (а) и L2 (б); PSD – *power spectral density function* (модификовано и преузето из [299])

У фокусу програма модернизације GPS-а, јесте увођење нових кôдова за рангирање. Тако, сигнал L1, биће проширен L1C сигналом, односно L1M, како би се повећала доступност сигнала за цивилне, односно војне кориснике [300]. GPS-ов L2P(Y) сигнал на 1227.6 MHz, користи се за прецизне војне примене. Цивилни корисници, могу користити овај сигнал на "безкодни" начин – пријемник најпре проналази L1 сигнал, а затим користи неке од информација L2 сигнала за побољшање тачности. Као и код L1 сигнала, модернизација GPS-а, приширује L2 сигнал на два, L2C и L2M. Сигнал L2C није велике прецизности, већ је јачи и спорији сигнал дизајниран да буде доступан у изазовнијим окружењима (овом сигналу GPS пријемник може приступити без претходног примања сигнала L1), док је други нови сигнал, L2M, доступан само овлашћеним корисницима.

Поред тога, GPS-ов сигнал **L5** на 1176,45 MHz, дизајниран је да испуни захтеве за безбедност у ваздухопловству [301] – L5 се емитује у радио-фреквентном опсегу резервисаном искључиво за **услуге безбедности у авио саобраћају**. Одликује се напредним дизајном, велике је снаге, пропусног опсега и брзине (као код прецизних кодова на L1 и L2); L5 сигнал је тренутно широко доступан (од 18 сателита) и очекује се да ће бити потпуно доступан (24 сателита) 2024. године [300]. Авиони ће користити L5 у комбинацији с L1 C/A за повећање тачности (јоносферска корекција), робустности (редунданса сигнала) и безбедности, као и капацитета и ефикасности у ваздушном простору. Иначе, емитовање поруке цивилне навигације (*Civil Navigation*, CNAV) на сигналу L5, почело је у априлу 2014. године. Међутим, L5 је и даље у пре-оперативној фази.

Брзина сигнала који се емитују са сателита мења се с променом растојања између сателита и пријемника (с приближавањем и удаљавањем сателита од пријемника) због Доплеровог ефекта. Промена брзине преноса директно је пропорционална промени фреквенције емитованих сигнала и промени удаљености између сателита и пријемника током одређеног временског интервала. Због тога сигнал, који емитује сателит с фреквенцијом L1, L2 или L5, а који прима пријемник, је различите фреквенције (око 5 KHz) у односу на емитовану са сателита, због кретања сателита у односу на пријемник, тј. Доплеровог ефекта. GPS пријемници компензују ове промене фреквенције.

Сваки GNSS сигнал, састоји од:

- Носиоца – радио-фреквентни синусоидални сигнал, који преноси информације о подацима на одређеном фреквенцијском опсегу, у циљу преношења информације кроз простор у облику електромагнетног таласа.
- Кôда опсега (кôд ширења) – подаци, тј. навигационе поруке, које сателит треба да преносе, су дигитални. Бројни сателити међусобно комуницирају истивремено. У пријемнику, за разлагање примљених сигнала у раздвојене сателитске сигнале, користе се различите технике, као што је техника широког спектра, тзв. многоструки приступ поделе кода (*Code Division Multiple Access*, CDMA)[134], тако да се подаци поруке с ниским нивоом преноса кодирају псеудослучајном секвенцом (*Pseudo Random Noise,* PRN) високог нивоа, а која се разликује за сваки сателит. На тај начин, GPS пријемник може разликовати сигнале, тј. PRN кодове, који долазе с различитих сателита; подаци поруке емитују се брзином 50 bit s^{-1}. Дакле, CDMA користи шему/образац битова псеудослучајног шума (PRN), који су јединствени за сваки сателит. Подаци и PRN-ови се комбинују и шаљу као аналогни сигнал. PRN је усклађен с једним од бројних кôдова рангирања (C/A кôд и P(Y) кôд). Избор овог кôда, утиче на особине PRN-а, података и аналогног сигнала. Да би се направила разлика између битова података и PRN битова, ови други се називају чиповима. Дакле, сателит емитује више од једног аналогног сигнала, од којих сваки има један или више PRN-ова који су услађени с различитим кôдовима рангирања. Тренутно се на фреквенцији L1 нуде и услуге *Standard Positioning Service* (SPS) и *Precise*

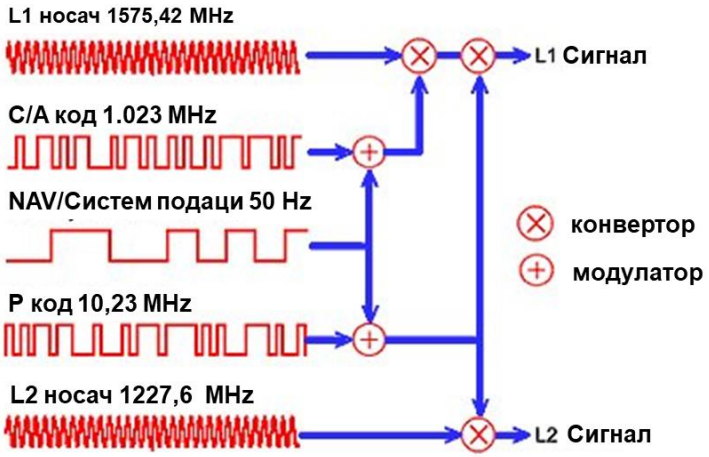
[134] У CDMA, сваком комуникатору се константно додељуе цео спектар. Вишеструке симултане трансмисије раздвајају се коришћењем теорије кодирања. CDMA издваја жељени сигнал и одбацује све остало као насумични шум.

Positioning Service (PPS), док се на фреквенцији L2, нуди само услуга PPS. SPS је услуга којој може приступити сваки цивилни корисник; заснован је на C/A кодном низу. PPS сервис доступан је само овлашћеним корисницима (војска); осим C/A користи и P кôд, што обезбеђује већу тачност одређивања локације.

Дакле, у употреби су два различита кодирања [302] (сл. 20), тј. два PRN кода, и то су: груби/аквизицијски (*Coarse/Acquisition*, C/A) kôd, тзв. златни кôд, на 1.023 MHz и прецизни (*Precision*, P(Y)) на фреквенцији 10,23 MHz.

Сигнали се модулирају на сигнал носача (преносиоца), L1 и L2, методом бинарног фазног помераја (*binary phase shift keying*), који кодира 1 *bit* по фазном помаку [303]. Носач L1 је модулисан са оба кода C/A и P, док је L2 модулисан само P кодом. Кôд C/A је доступан/јаван и користе га цивилни GPS пријемници. Међутим, P кôд може бити криптован, и једино је доступан војној опреми уз одговарајући дескрипциони кључ.

- Навигационе поруке – даје детаљне податке и информације стању сателита, ефемеридама (подаци о орбитама) сателита, алманаху, и додатне компламентарне информације [304].



Слика 20. Структура GPS сигнала (модификовано и преузето из [271])

Техничке карактеристике GPS фреквенцијских опсега L1, L2 и L5 сумарно су дате у Табели 5. Свакако, L1 је најчешће глобално коришћени GPS, који функционише на фреквенцији 1575,74 MHz, којој се приступа преко CDMA-а. Садржи три различита сигнала: груби/аквизициони (C/A) кôд, P кôд и M кôд. Кôд C/A је најприхваћенији и најважнији кôд, и као што је претходно поменуто, намењен је цивилној употреби и на употреби овог сигнала, ослањају се бројна решења развијена на тржишту за коришћење GPS система; дужина сигнала/кôда је 1 ms при брзини чиповања од 1023 Mbps (Mbs^{-1}) [305]. Прецизни P кôд намењен је само војне примене. P(Y) кôд често замењује P кôд, при коришћењу анти-спуфинг система. Дужина овог сигнала/кôда је 7 дана (при брзини чиповања од 10.23 Mbps), која обезбеђује поверљивост и аутентификацију. Трећа врста кôда, тј. M кôд, дизајниран је искључиво за војну употребу и може евентуално заменити P и

P(Y) кôд. Има боље карактеристике – отпорнији је на ометање и обезбеђује боље перформансе и већу флексибилности од P(Y) кôда.

Табела 5. Техничке карактеристике GPS фреквенцијских опсега L1, L2 и L5 [287, 306]

Фреквенцијски опсег	L1			L2	L5
Кодови рангирања	C/A	P(Y) код	M код	P(Y) код	
PRN					
Дужина кода	1023	$6{,}19\times10^{12}$	Криптографски генерисан	10^{12}	10 230
Брзина чиповања (Mbps)	1023	10,23		0,5115	10,23
Аналогни сигнал					
Фреквенција носача (MHz)	1575,42	1575,42	1575,42	1227,60	1176,45
Модулација	BPSK*	BPSK	BOC_{sin}**	BPSK	BPSK
Сервис	SPS	PPS	PPS	PPS	SPS

* BPSK – *Binary Phase Shift Keying* [307, 308]
** BOC_{sin} – *Binary Offset Carrier signals* (*sine-phase*) [309]

Као и у претходном периоду [310], међународне организације, ICAO и EUROCAE, развијају стандарде за следећу генерацију GNSS-а у цивилној авијацији и промовишу дискусије о еволуцији улоге овог система у ваздухопловству, и паралелно с тим, подстичу неопходни техничко-технолошки развој [311, 312]. У вези с тим, ICAO је 2018. године објавила [313] верзију концепта операција за употребу *Dual-Frequency Multi-Constellation* (DFMC) GNSS у авијацији, док је *Minimum Operational Performance Standard* (MOPS) за GPS и Galileo на фреквенцијским опсезима L1/E1 и L5/E5a, у процесу дефинисања. Очекивано је да ће DFMC GNSS заменити једнофреквентни GPS L1-C/A у будућим регулативама за цивилно ваздухопловство. Такође, еволутивни концепти, који обухватају проминентну улогу GNSS-а су нпр. *Advanced Receiver Autonomous Integrity Monitoring* (ARAIM) систем [314], затим, *Airbone Separation Assurance System* (ASAS) [315], као и *Multi-dimensional trajectory management* [316].

Дакле, тренутни статус GPS-а је његова модернизација [317], а у фокусу је додавање три нова навигациона цивилна сигнала (L5, L2C, и L1C) сателитској констелацији, тако да ће уз ″стари″ L1 C/A цивилни сигнал (који ће наставити да се емитује), бити на располагању укупно четири цивилна GPS сигнала (L1 C/A, L5 и L1C), у фреквенцијским опсезима додељеним за *aeronautical radio navigation services* (ARNS). SBAS-ови, као што је *Wide Area Augmentation System* (WAAS) у Северној Америци, еволуирају тако да подрже дво-фреквентну корисничку опрему. Поред тога, распоређене су и друге констелације језгра GNSS-а (руски GLONASS) или су већ распоређени (европски Galileo и кинески BeiDou). ICAO *Navigation*

System Panel ажурира стандарде и препоручене праксе (SARPs) садржане у Анексу 10 Међународне конвенције о цивилном ваздухопловству ICAO [283], за инкорпорирање модернизације GPS-а и GLONASS-а, као и нове констелације сателита. Стандарди за авио-опрему су/биће потребни за безбедно коришћење. GPS/GLONASS L1 MOPS је дефинисан и усвојен (2017), као први корак у стандардизацији мулти-констелационе опреме.

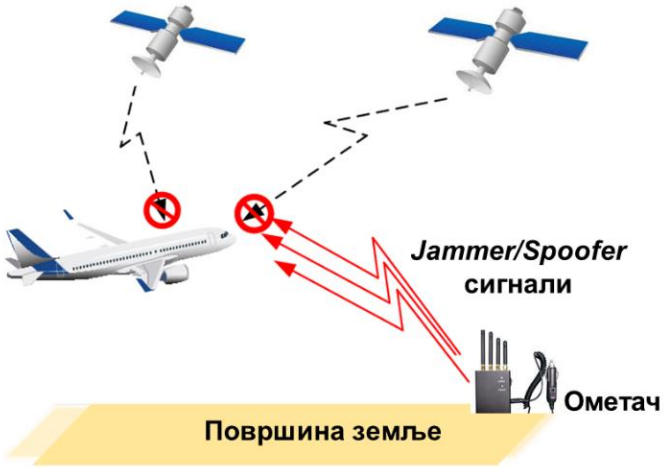
5.2. САЈБЕР БЕЗБЕДНОСТ GPS/GNSS-а

Због широко распрострањене употребе GPS/GNSS-а, у фокусу су истраживања у вези са безбедношћу GNSS система, тј. рањивостима овог система. У авио-сектору, ваздухопловни системи, засновани на сателитској навигацији (*Satellite Navigation,* SatNav) као што су GPS/GNSS или ADS–B, а с обзиром на то да имају веома једноставан безбедносни протокол, који не обезбеђују потпуну аутентификацију и енкрипцију податка, рањиви су на различите врсте сајбер напада, као што је нпр. спуфинг (*spoofing*) (део 2.1.2), један од облика намерних радио-фреквенцијских сметњи (*radio frequent interference,* RFI), а који је веома опасан и представља велики ризик по функционисање GPS система. Осим *spoofing*-а, у овом делу биће описани и друге врсте сајбер напада на GPS (детаљно разматрани у делу 5.2.1), као и предложене одбрамбене стратегије за ублажавање сајбер рањивости (део 5.2.1.1), које обухватају широки спектар предлога, од коришћења физичких уређаја, преко криптографских техника процесирања сигнала, до техника верификације навигационих и временских параметара.

Дакле, веома велику пажњу и забринутост изазивају рањивости [228] GNSS-а у вези са RFI, тј. инцидентима нестанка GPS сигнала у авионима цивилне авијације, и то нарочито у географским подручјима с политичким тензијама (нпр. Југоисточно Средоземље, правци Блиски истик–Канада и САД преко Северног пола кроз руски ваздушни простор) или у близини одређених аеродрома. Као што је дискутовано, различити су узроци ових инцидената, као нпр. соларне олује, војне вежбе, али исти могу бити и намерно изазвани [318].

Различити сајбер инциденти/напади у авијацији су реалност, а међу њима су и они који се односе на сајбер сметње GNSS-а. Број ових инцидената, расте великом брзином, као што се повећавају и начини за овакве сметње, према извештајима IATA и EUROCONTROL у вези са безедношћу GNSS-а [319, 320]. Најскорије, објављени инциденти у вези са ометањем рада GNSS су нпр. GPS инциденти на једном аеродрому у Манили на Филипинима (2016), када је у периоду од 3 месеца, пријављено више од 50 GPS сметењи [321]. Затим, сметње на GPS пријемницима у авионима Норвешке компаније, близу границе с Русијом [322], као и северној Финској током војне вежбе NATO-а [323], само су неки од познатих инцидената у вези са GPS ометањима. Такође, у прилог тврђењу о значајном порасту ових инцидената, јесте и чињеница да је у периоду од 3 године (2014–2017), било око 50 пута више прекида/сметњи у функционисању GPS-а [320], и то углавном изазваних лажирањем (*spoofing*) и ометањем (*jamming*) GPS сигнала (сл. 21). Сценарио ових врста напада, нпр. заснива се постојању ометача (О, на Земљи), који шаље сигнале, а који су у фреквенцијском опсегу GNSS пријемника у авиону – при великој снази

ових сигнала, због интерференција, сателитски сигнали (испрекидана линија, сл. 21) биће поништени/угашени, и пријемник у авиону неће добити GNSS сигнале.



Слика 21. Интерференције GNSS-а у случају напада са Земље (модификовано и преузето из [228])

Систем за навигацију је основни, веома важан део авио-система, који омогућава континуирано лоцирање и праћење авиона, како са Земље, тако и из ваздуха (авиона). У савременим авионима, главне навигационе технике, биће сателитске, тј. оне које се заснивају на сателитским системима, као што су SBAS и GBAS (део 5.1). Док се ваздухопловна индустрија и даље ослања на конвенционалне инструменте, тзв. навигациона средства (*NavAids*), као што су DME, ILS и VOR (поглавље 3.1), напрецизнија технологија навигације данас, јесте технологија сателитске навигације. Међутим, последица мале снаге *SatNav* система, а нарочито, сигнала GNSS навигационог система, као што је поменуто, је њихова рањивост/слабост на RFI. Тако, коришћење уређаја за ометање[135], који емитује RF таласе мале снаге (10 dBm) може блокирати GNSS сигнал у радијусу од 100 m, док преносиви ометачи, могу пореметити пријем GNSS сигнала на удаљеностима од десетине километара.

Број ненамерних ометања GNSS-а се повећава, а последице ових инцидената су недоступност навигације која се заснива на GNSS-у (као нпр. ADS–B система, део 6). Тренутно, ублажавање ових сметњи/рањивости у комерцијалној авијацији, заснива се на коришћењу авионске опреме, тј. *on-board* авионике, која обезбеђује мање прецизну резервну навигацију, као и имплементација додатних решења [228].

Друга, много опаснија врста интерференција у *SatNav* системима је лажирање (*spoofing*, спуфинг), изазвано ненамерно или намерно (злонамерно). У овом случају,

[135] Генерално, уређаји за ометање могу имати различите облике и величине, а најчешће су то преносиви, тј. мобилни уређаји. Ометачи за цивилну употребу, иако малих димензија, мале потрошње енергије, чије се батерије могу напајати у аутомобилима, могу ометати пријем GNSS сигнала на великим удаљеностима (око 10 km). Ометачи који се користе у војне сврхе (јединице за сајбер ратовање), најчешће су ометачи велике снаге, који се постављају на возила, и који могу обухватити и неколико хиљада километара [324].

као што је објашњено у делу 2.1.2, се емитују/примају фалсификовани GNSS сигнали, што значи да спуфер, користећи лажни сигнал (уместо истинитог, који шаље сателит), може нпр. преусмерити авион на погрешну руту и тако изазвати веома велики безбедносни ризик. Наиме, у спуфингу, предајник (*spoofing devices*) шаље лажни GPS сигнал пријемнику–мети, у сврху продукције лажних информација (погрешно позиционирање или временско одређење), а уколико пријемник нема могућност разликовања аутентичних сигнала од лажних, онда није ни у могућности да упозори корисника на непоуздану навигацију. За имплементацију спуфинга, могу се користити различити уређаји/алати, као што је јефтини и широко доступан спуфинг уређај – *Software Defined Radio,* SDR[136] који, поједностављено речено, ″може натерати паметни телефон да мисли да је на Монт Евересту″ [325]. Дакле, последица *spoofing*-а је погрешна информација (губитак интегритета поруке), што је много опаснија и озбиљнија интерференција, у односу на ометање (*jamming*) GPS сигнала [326].

Пријављени инциденти у вези с овом врстом интеференција у ваздухопловству, још увек су веома ретки, а до недавно, став цивилног авио-сектора у вези са GNSS спуфингом, био је ограђивање од проблема и став да је питање спуфинга у делокругу војних, а не цивилних структура [311]. Међутим, како су све више у фокусу уобичајене RFI, тако је и став према спуфингу еволуирао, што је делимично узроковано инцидентом [327, 328] који се догодио у Немачкој, на аеродрому у Хановеру (2010), а који је био изазван RF сметњама GPS репетитора и узрочно неадекватним позиционирањем GNSS система. Познато је да постоје бројне међуфазе спуфинга, од погрешног позиционирања репетитора, па све до оног што би могла урадити нека малициозна, али вешта особа, коришћењем неког спуфинг уређаја, као што је SDR [329]. Због свега тога, на ову врсту претње треба обратити нарочиту пажњу, као и на развој и примену адекватних анти-спуфинг техника за ублажавање рањивости GNSS система на спуфинг претње.

Иако су различити делови авио-система изложени различитим врстама сајбер напада, а потенцијално и спуфингу, као што је претходно дискутовано [14, 15], постоје одређена **безбедносна решења**, препоруке и протоколи дефинисани од стране ICAO, RTCA и EUROCA, које, заједно с различитим радним групама, конференцијама и организацијама, на националном, као и међународном нивоу, континуирано прате и евалуирају предложене антиспуфинг детекционе методе/технике и њихову интерграцију у системе за комуникацију, навигацију и надзор. Тако, један од циљева које је поставила RTCA у вези са авио-опремом следеће генерације, јесте заштита од RFI, тј. повећање сигурности GNSS-а на безбедносне ризике у присуству RFI, укључујући и спуфинг. Такође, актуелни правци у решавању рањивости на спуфинг, постављени од стране RTCA и EUROCAE, првенствено се односе на увођење нових захтева за детекцију спуфинга GNSS-а, а то значи и коришћење алтернативне невигационе опреме, која нема значајне безбедносне ризике [20].

[136] SDR је софтверски дефинисани радио, тј. комуникациони систем у коме функције, као што су подешавање, филтрирање, модулација, демодулација, обавља софтвер (уместо хардвера), као постигнуће напретка у развоју дигиталне електронике. Доступност и континуирано смањење цене SDR, утичу на пораст употребе ових уређаја.

5.2.1. Сајбер рањивости GPS/GNSS -а

Радио-фреквенцијске интерференције (**RFI**), као што је претходно поменуто, могу деградирати цивилне GNSS сигнале и сервисе, и представљају реалну опасност, с обзиром на константан пораст употребе IoT (фусноте 23, 27 и 43) [47], GNSS репетитора, SDR картица, и очекивану, широку употребу софистициранијих спуфинг уређаја у будућности.

Према *International Telecommunication Union* (ITU), RFI представља ″утицај нежељене енергије изазване емисијом или комбинацијом емисије, зрачења или индукције на пријемник радио-комуникационог система, који се манифестује погоршањем перформанси, погрешним тумачењем или губитком информација″ [330].

RFI се деле, према извору сметње, на **природне**, које су последица различитих ефеката бежичних канала, и **вештачке**, које производе различити бежични предајници.

Природне интерференције/сметње су последица интеракције RF таласа и препрека на бежичним каналима, тј. различитих оптичких појава, као што су рефлексија, дифракција, рефракција, расипање, сцинтилација, итд. Као последице ових појава, може доћи до вишеструке дисторзије RF (вишеструко ширење, *multipath propafation*) сигнала (сигнали стижу до антене пријемника из различитих праваца, тј. преко неколико путева), затим, кашњења/слабљења сигнала услед рефлексије и рефракције таласа у јоносфери и тропосфери, као и сцинтилација сигнала (ефекат метеоролошких услова у јоносфери). Облици природних интерференција су и деструктивне сметње (блеђење, *fading*), сенчење (*shadowing*) и Доплеров ефекат на бежичним каналима, што може довести до тога да RF сигнал буде веома мале јачине у одређеним областима, као и фазно померен.

Вештачке интерференције/сметње, могу бити намерне и ненамерне, у зависности од тога да ли су генерисане злонамерним предајником, или не. **Намерне** сметње обухватају *jamming* (ометање) и *spoofing* (лажирање). **Ненамерне сметње** се деле на сметње на истом каналу (изазване емисијом предајника који користи исти канал, као нпр. проблем алокације радио ресурса или унакрсног разговора), и сметње суседног канала (последица RF емисије из једног канала у други код нпр. интермодулационих производа). Бројни су извори ненамерних сметњи („ометачи“) на GNSS, узроковне различитим RF системима/електричним уређајима, који емитују хармонијске фреквенције блиске фреквенцијама GNSS сигнала, као што су хармоници VHF комуникација, телевизијске станице, неке врсте радара, војни системи, итд. Такође, осим у авијацији, GNSS се користи у многим другим апликацијама различитих сектора, као што је железнички транспорт, пољопривреда, метеорологија, итд. Ометање (намерно), усмерено на кориснике ван авијације, може утицати на авио-сектор индиректно, или директно, када се уређај за RFI намерно користи за ометање објеката ваздушне навигације који зависе од GNSS-а, коришћењем персоналних уређаја као ометача или предузимањем намерних напада на авио-сектор [331].

С обзиром на то да се интерференција може дефинисати као сваки поремећај електронског система/уређаја услед спољашњих електромагнетних емисија на

актуелну/од интереса радио-фреквенцију [228], она имплицитно обухвата и најштетније облике RFI, и то су: ометање (*jamming*) и лажирање (*spoofing*).

Jamming (ометање) односи се на емисије сигнала, које ометају пријемник (али не имитирају GNSS сигнале), тј. на интерференције, које деградирају пријемник (смањују способност пријемника за примање и праћење GNSS сигнала).

Spoofing (лажирање)[137] односи се на емитовање сигнала сличних GNSS сигналима, који се могу прикупљати и пратити у комбинацији с легитимним сигналима, или уместо њих. Тако се у пријемник – мету (″жртву″) убацују, тј. подмећу лажни сигнали у циљу погрешног PVT. Због тога је *spoofing* много суптилнији и опаснији облик претње на GNSS, у односу на *jamming*. Међутим, сматра се да је остваривање спуфинг напада, у односу на ометање, мање вероватноће, јер је његово извођење технички много сложеније. Међутим, с обзиром на то да GPS цивилни сигнал није шифрован и енкриптован [291, 302] (део 5.1.1), потенцијалним спуферима није тешко/скупо да израде спуфинг уређај за подметање лажних (уместо аутентичних сателитских) сигнала примаоцу – мети; слањем ових сигнала на GNSS пријемник, може доћи до ″закључавања″ пријемника на лажне сигнале, уместо на аутентичне сателитске сигнале. Дакле, у неким спуфинг нападима, може доћи до престанка рада GNSS пријемника (″закључавање″ пријемника услед аномалија у подацима), иако нема RF преоптерећења [311]. Иако су веома ретки потвђени извештаји о експлоатацији спуфинга у цивилној авијацији, техничка изводљивост ове врсте напада је реална, а потенцијал велики. Поред тога, готово сваки уређај чији се рад заснива на коришћењу цивилног GPS сигнала, рањив је на спуфинг [332], а примена спуфинга постаје флексибилнија и јефтинија, услед брзог развоја SDR платформи.

Категоризација RFI, као и детаљна дискусија о различитим врстама сајбер претњи на GNSS систем, дата у прегледном раду [228], као и радовима [149, 333], омогућава анализу различитих сценарија напада на GNSS, као и за тестирање перформанси предложених техника за ублажавање рањивости GNSS-а на RFI у авијацији [333].

Још од почетка развоја и примене GPS-а [334] RFI биле су у фокусу проучавања, а US *Department of Transportation* (USDOT), извршило је (2001) детаљну анализу и процену утицаја RFI на GPS у критичним инфраструктурама, укључујући и ваздухопловну индустрију, што је имало за резултат повећање свести о значају и последицама ових интерференција, тј. поремећаја функционисања GPS-а. У извештају USDOT, тзв. Волпеовом извештају [271], *spoofing* је означен као много опаснији облик RFI од намерног ометања (*jamming*), с обзиром на то да код спуфинга актуелни пријемник не може открити напад, нити упозорити корисника на непоуздана навигациона решења. Штавише, и ако је делимично успешан, ињектирањем погрешних информација у циљани пријемник, спуфинг проузрокује значајне PVT грешке. Због тога ће ова врста RFI бити детаљније описана у наредном делу дисертације.

[137] Посебан случај спуфинга, јесте *meaconing*, који се односи на поновно емитовање (тј. ″копирање″) аутентичних навигационих сигнала од стране злонамерног предајника [228, 288].

5.2.1.1. Врсте безбедносних претњи на GPS/GNSS – *spoofing* у авијацији

У авијацији, спуфинг је све више у фокусу истраживача из области авио-сајбер безбедности, због велике штете (непосредне и посредне) коју може нанети авио-системима, као и због тога што употреба спуфинга постаје све флексибилнија и јефтинија [335], услед веома брзог напредка SDR технологија (фуснота 136). Поред тога, анализа различитих сценарија спуфинг напада, значајна је и за развој техника/метода за детекцију и ублажавање спуфинг напада, како би се повећала сигурности и безбедности система ваздушног саобраћаја.

Свакако, постоје **различити облици спуфинга**, а сврсисходно је класификовати и дефинисати типичне/репрезентативне облике спуфинга у циљу њихове анализе и тестирања перформанси различитих анти-спуфинг техника у авијацији. Спуфинг напади могу се класификовати на различите начине, као нпр. на основу карактеристика спуфинга (синхронизовани и несинхронизовани, у зависности од тога да ли је лажни сигнал синхронизован или није с аутентичним GNSS сигналима), затим, према нивоу сложености [336] (поједностављене, интермедијерне и софистициране), као и интенцији напада (спуфинг напади, S1–S7, Табела 6) [333, 337].

Табела 6. Категоризација спуфунг напада [333]

Врсте спуфинга
S1 – Понављање (*Repeaters*)
S2 – Погрешни сигнали (*Errant Signals*)
S3 – Колатерални спуфери – симулатори (*Collateral Spoofers – Simulators*)
S4 – Колатерални ре-емитујући спуфери (*Collateral Re-radiating Spoofers*)
S5 – Циљани спуфери – Симулатори (*Targeted Spoofers – Simulators*)
S6 – Циљани ре-емитујући спуфери (*Targeted Re-radiating Spoofers*)
S7 – Циљани софистицирани спуфери (*Target sophisticated spoofers*)

Карактеристике **спуфунг напада** класификованих према нивоу сложености су следеће [333, 337]:

- *Поједностављени спуфинг напади* – могу се извести коришћењем неке врсте GNSS симулатора (генератор GNSS сигнала повезаног са антеном предајника) за добијање фалсификованих GNSS сигнала. Пријемник (у моду праћења) може бити преварен, тј. добити лажни сигнал, када изгуби пријем сигнала са сателита, тако да се може "закључати", тј. прећи на режим пријема спуфинг сигнала. Постоји могућност да ометач доведе до тога да пријемник изгуби "закључани" сигнал са сателита, и тако доведе до поновне реаквизиције сателита. Најчешће, сигнали нису синхронизовани са оригиналним сигналима, ни фазно (PRN-кôдна фаза) нити Доплеровом фреквенцијском померају, што омогућава употребу једноставних COTS компонената (фуснота 52). Међутим, извођење напада може бити и прилично скупо, с обзиром на то да захтева коришћење специфичног, скупог хардвера, који није лако преносив. Детекција напада је релативно једноставна – због одсуства синхронизације сигнала (лажног и оригиналног),

долази до наглог пораста излазних сигнала, који се односе на положај и време. Такође, при великој јачини спуфинг сигнала, пријемник за мониторинг може потенцијално детектовати повећану активност у GNSS фреквенцијским опсезима.

- *Интермедијерни спуфинг напади* – сложенији напади од претходно описане врсте, и за разлику од њих, фалсификовани GNSS сигнали су синхронизовани са оригиналним GNSS сигналима, који долазе са сателита, тј. спуфер може синхронизовати фреквенцију и ускладити фазу кôда између првог и фалсификованог сигнала. Пријемник нападача праћењем сигнала са сателита, има познату локацију (и путању) пријемника – мете, релативно у односу на антену пријемника, што омогућава да се лажни, псеудо-сигнал ″поравна″ са аутентичним кодовима на позицији пријемника – мете. Када је пријемник у режиму праћења, а на почетку напада, лажни сигнали веома су добро усклађени са аутентичним, тако да постепеним повећавањем јачине и сукцесивним подешавањем сигнала, спуфер може симулирати нивое сигнала компатибилне са сателитским, и тако преузети контролу. Како спуфер тачно репродукује фазу кôда, фреквенцију и навигационе податке, пријемник авиона не може разликовати лажни сигнал од оригиналног. Дакле, детекција на пријемнику – мети готово је немогућа, осим у случају када се за процену смера доласка сигнала користи већи број антена. Генерално, сваки GNSS пријемник, адекватно модификован, може бити коришћен за извођење ове врсте спуфинга. Софтверски делови и RF компоненте за израду спуфинг уређаја су доступне на тржишту, али је за дизајнирање спуфинг уређаја, неопходно значајно познавање структуре и обраде GNSS сигнала. У контексту цивилног ваздухопловства, за сада, оваква врста напада је мање вероватна, због тога што нпр. синхронизација лажног и оригиналног сигнала захтева гломазну *on-board* опрему за пријем, обраду и ре-емитовање фалсификованих сигнала, као и због тога што је за његову реализацију потребно да монитори за ометање и лажирање GNSS-а, требало би да буду инсталирани и активни у подручју аеродрома.
- *Софистицирани спуфинг напади* – сложенија верзија интермедијерног спуфинга, који представља координисани и синхронизован напад извршен различитим уређајима за лажирање [338]. Дакле, код ових напада, могли би се користити вишеструко координисани „интермедијерни спуфери“ за реплицирање садржаја, као и ″поравњање″ GNSS сигнала и њихове просторне расподеле. Овај облик спуфинга теже се детектује, Међутим, слично као код интермедијерног спуфинга, алоцирани (на другој локацији) надзорни пријемник ће, у случају софистицираног спуфинга, имати нагло повећање вредности излазних сигнала, који се односе на положај пријемника и време, с обзиром на то да ли је положај алоцираног пријемника различит од положаја пријемника – мете. Затим, уколико су лажни сигнали велике јачине, онда алоцирани пријемник за надзор, потенцијално може детектовати повећану активност у GNSS фреквенцијским опсезима. Ова врста напада је веома комплексна и скупа за имплементацију, као и тешко изводљива, јер се нападима, који се базирају на више посредних лажирања, веома тешко управља. Због тога, у контексту цивилног ваздухопловства, сматра се да је вероватноћа оваквог напада веома мала, због техничке сложености имплементације и логистичких проблема, и то

нарочито у динамичким сценаријима (нпр. уређаји за лажирање делују као антенски низ за формирање снопа који симулира различите углове долазних сигнала за различите сателите, што се постиже или фиксирањем сваког спуфера и преношењем сигнала свих сателита с одговарајућим кашњењима компатибилним с антеном пријемника, или тако што сваки спуфер емитује сигнал тачно једног сателита и механички померајући спуфер око пријемника – мете).

Подела спуфинга према особинама напада, као и интенцијама спуфера [333], која прави разлику између колатерала, циљаног и софистицираног спуфинга, дата је у табели 6. Израз колатерал се односи на ситуацију у којој ваздухоплов није намерна мета интереференција, а лажни сигнали (положај, снага и сл.), највероватније нису синхронизовани с оригиналним сигналима пријемника (антена), тако да је очекивано нагло повећање/смањење карактеристика сигнала (положај, опсег и јачина). Израз циљани, користи се када је један, или су више ваздухоплова мете, тј. када су RF емисије намењене да нарочито утичу на авион/е; у овом случају, ометајући сигнали су синхронизовани (усклађени) с аутентичним сигналима, тако да нису једноставно уочљиве грешке на пријемнику. Израз софистицирани, користи се у случајевима веома тешке детекције ометајућег сигнала, као нпр. у случају вишеструких сигнала, који се емитују из различитих праваца.

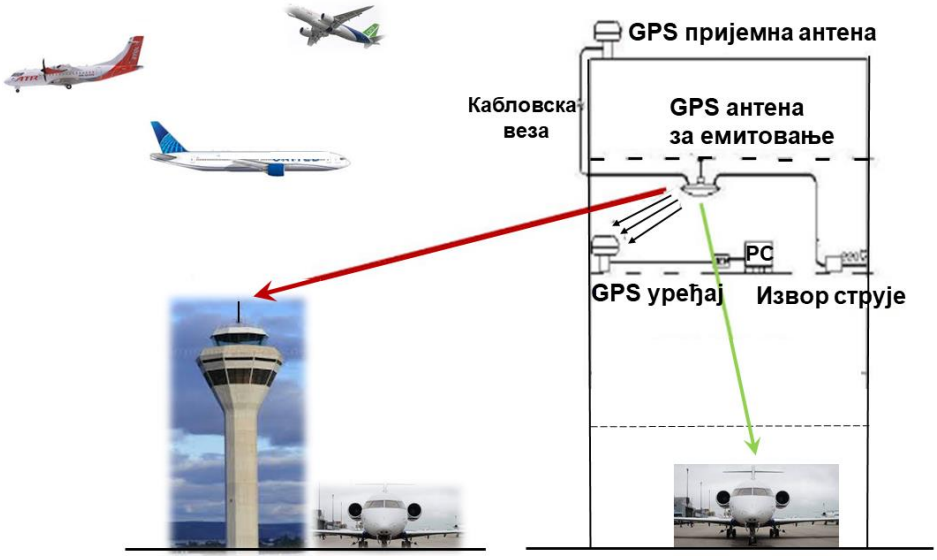
Подела спуфинга дата у Табели 6 (спуфинг напади S1–S7), на основу декларисања циља – мете спуфинга, веома је сврсисходна као подстицај дискусије о начинима имплементације спуфинга (с техничког аспекта) у постојеће авио стандарде, и нарочито у поступцима анализе/провере GNSS пријемника, тј. постављање захтева које мора испунити кориснички пријемник.

Различите врсте спуфинг напада [333], приказани су на сл. 22 (а и б), и то, спуфинг напад S1 – Спуфинг понављањем (сл. 22 а), као и S5 – Циљани спуфери – Симулатори (сл. 22 б). Спуфинг S1 одговара поједностављеном спуфинг нападу, као нпр. у случају погрешно постављених или конфигурисаних GNSS репетитора (користе се за аквизицију сигнала пријемника у аеродромским хангарима), емитују сигнале који могу спуфовати пријемнике авиона. Спуфинг S5 одговара интермедијерном спуфинг нападу, у циљу спуфинга авио-пријемника, тако да емитовани сигнали морају бити усаглашени са сигналима које прати авион. Иницијално могу имати усклађене грешке у позиционирању, а претходи им ометање, како би се пријемник – мета пребацио на спуфоване сигнале. Овој врсти припадају спуфери који ињектирају нетачне/неважеће дигиталне податке, што може резултирати бројним ризичним ефектима, од погрешних PNT до неадекватног рада пријемника. Ефекат ових напада може бити тренутан или одложен, али и дуготрајан. Изводи се коришћењем једног предајника, дизајираног или комерцијално набављеног с ограниченим/јефтиним ресурсима и опремом.

Као што је претходно дискутовано, GNSS није једино навигационо средство у авијацији (поглавље 3.1); пилоти/авиони информације добијају и од других навигационих система, као и од визуелних референци. То имплицитно значи да, чак и у случају успешног софистицираног спуфинг напада, који није ублажен у GNSS пријемнику, пилот може, у већини ситуација, ублажити ефекте напада, тј. значајно

их смањити. С друге стране, пилоти не могу указати/пријавити спуфинг, због чињенице да се спуфинг не може тренутно детектовати, или пратити (надгледати) у авиону. Због тога је од кључне важности да будући авиони имају могућност детекције, локализације, ублажавања и евентуално разликовања присуства ометања и спуфинга.

(а)



(б)

Слика 22. Различите врсте спуфинга: (а) S1– Спуфинг понављањем и (б) S5– Циљани спуфери – Симулатори (модификовано и преузето из [333])

За компензацију јачине флуктуације GNSS сигнала, користи се *Automatic Gain Control* (AGC). Наиме, **AGC** је адаптивни појачивач, чија је основна улога синхронизација примљеног сигнала (амплитуде сигнала) с улазним пропусним опсегом аналогно-дигиталног претварача (*Analog-to-Digital Converter*, ADC), у циљу минимизирања губитака у јачини сигнала. Како у GNSS пријемник стижу сигнали мале јачине, који могу бити прекривени сигналом термалног шума, тако да се при јаким сметњама, амплитуде сигнала повећавају, резултујући засићењем ADC-а. Да се то не би догодило, AGC смањује појачавање сигнала и спречава засићење ADC-а. С друге стране, присуство варијација у појачању AGC-а, драгоцен су показатељ присуства интерференција. Дакле, AGC доводи до рањивости пријемника на спуфинг [339]. Поред тога, пријемник не може утврдити одакле се емитује сигнал, тј. да ли је предајник легитиман извор, или је локално генерисан извор лажних сигнала, јер је антена пријемника најчешће фиксирана у простору – уколико пријемник сигнала није заштићен, лажни сигнал може се директно убацити коришћењем спуфинг уређаја. Јенда варијанта је да, уколико спуфер познаје тачну локацију пријемника – мете, се лажни сигнали могу суперпонирати на аутентичне сигнале. Алтернативно, могу се користити и несинхронизовани лажни сигнали веће јачине, међутим, ова врста спуфинга је ефикасна у случају када је пријемник у фази пријема сигнала (иницијалној фази рада) или када је ″насилно откључан″ ометајућим/лажним сигналом.

Поменути случај **ометања GPS-а на аеродрому** у Хановеру (2010), пример је реалног спуфинга (ненамерног) [327]. Наиме, авион, који се налазио у близини прага писте, а чији су авио-системи функционисали по GNSS сигналима репетитора за тестирање авио-система авиона за пословну авијацију у хангару близу писте, имао је приказ погрешне GPS позиције током фазе таксирања и полетања. Иако једноставан, овај сценарио, може се користити као полазна основа за тестирање GNSS пријемника или било ког хардвера, који зависи од прецизног позиционирања или временских података, а које даје пријемник.

Други пример реалног ометања GPS-а је **прекиди рада** (2010) **GPS** пријемника на земљи (коришћени за асистирање GPS пријемницима у авиону, који је у прилазу), током FAA инсталирања новог система за слетање авиона заснованог на GPS-u (Интернационални аеродром *Newark*, USA). Истрагом је утврђено је да су узрок ових сметњи биле *personal protection devices* (PDDs) [340]. И раније је било пријављено FAA-у (јул, 2003) слично ометање/прекид функционисања три различита GPS пријемника. Узрок је био укључени мобилни телефон, који је проузроковао потпуни прекида рада GPS пријемника – сва три пријемника користила су три различите антене, које су инсталиране на малом авиону, а мобилни телефон је био укључен (без остваривања позива) током инцидента, као и у накнадним тестирањима [341]. Сви поменути инциденти указују на то да је детекција, односно тренутно упозорење на спуфинг GNSS, неопходна против-мера у циљу обезбеђивања безбедности и сигурности аеродрома.

Рањивост авио-система на спуфинг, узрокује и употреба GNSS-а у авио-операцијама слетања и полетања ваздухоплова. Поред ILS-а (поглавље 3.1), који користи већина ваздухоплова у комерцијалној авијацији, у порасту је и употреба GBAS система (поглавље 5.1), и то нарочито у Европи и Русији. Међутим,

сертификовање овог система, као међународног стандарда у цивилној авијацији успорено је, с обзиром на то да систем није аутентификован, и стога се може спуфовати. Наиме, већина GBAS пријемника лоцирана је на Земљи, тј. аеродромима, тако да постоји могућност спуфовања алтитуде авиона, што представља озбиљан ризик и може потенцијално довести до удеса. Затим, ометања (случајна или намерна) GNSS пријемника у авиону при авио-операцијама прилаза или одлета, могло би се остварити релативно једноставно и довести до удеса с трагичним последицама. У прилог томе говори инцидент ометања GPS-а (2009) који се догодио на *Newark Liberty* Интернационалном аеродрому (USA) током тестирања GBAS система [342], када су детектоване повремене и непредвидиве сметње, због чега су искључене земањске станице. Разлог сметњама били су мали GPS ометачи, које су користили возачи камиона да би онеспособили уређаје за праћење постављене од стране ауто-превозничких компанија. Тако су индиректно, тј. ненамерно изазвали прекид рада GBAS система и одложили сертификацију овог система за инструментално слетање.

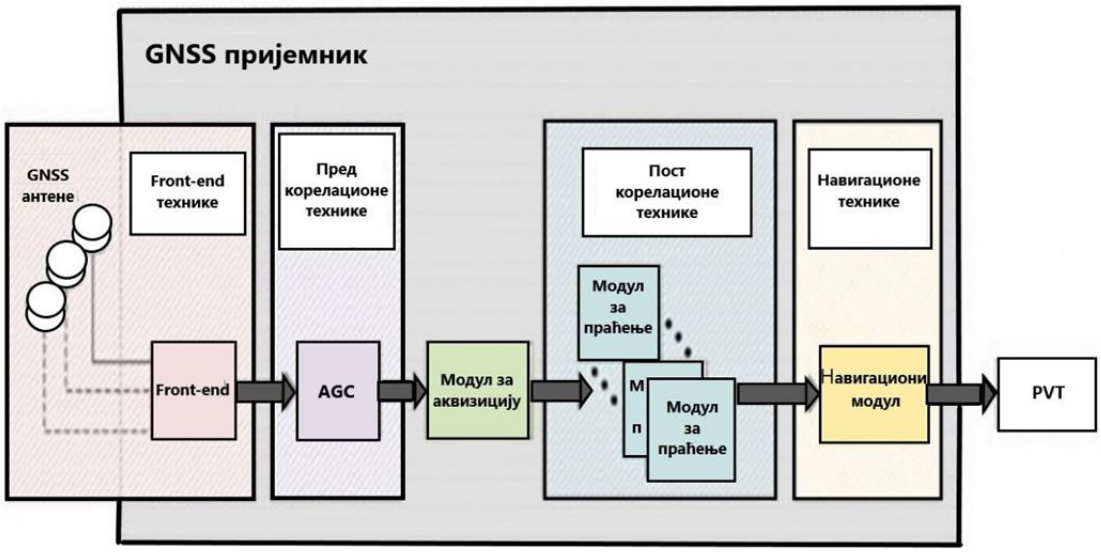
У авио сектору, специфични захтеви који се односе на снимање свих GNSS података, а који су релевантни за функционалност GNSS-а, детаљно су предочене у смерницама ICAO-а [343]. Држава, као водећи ауторитет, одобрава операције, које се заснивају на GNSS-у и требало би да обезбеди евидентирање GNSS података релевантних за операције засноване на GNSS-у, као и да подржава периодична тестирања и потврду да су карактеристике ових података (тачност, интегритет, континуитет и доступност) у захтеваним границама за одобрене операције. Тако, неопходно је да ATC и службе које обезбеђују услуге контроле прилаза, располажу подацима, тј. информацијама о оперативном статусу радио-навигационих система, а који су од круцијалног значаја за навигацију, тј. прилаз, слетање и полетање авиона. Свакако, перформансе свих система за навигацију морају бити у складу са захтевима (ICAO GNSS *Signal in Space Performance Requirements)* [343], а у којој мери навигациони систем задовољава прописане вредности, детерминише и врсту операција које се могу извршити.

5.2.2. GNSS стратегије за ублажавање сајбер рањивости

Као што се схватило још од почетка дизајнирања GPS-а, због веома мале јачине сигнала које GNSS пријемник (антена) добија од сателита, исти је рањив, тј. подложан интерференцијама/сметњама (ненамерним или намерним), како је и формализовано у Волпеовом извештају (2001) [271]. Поред тога, актуелна GNSS одобрења за коришћење стандардизованог једнофреквентног опсега, поједностављују намерна/ненамерна ометања GNSS сигнала. Шта више, као што је претходно поменуто, GNSS је рањив на RFI, укључујући и природне интерференције, тј. поремећаје у јоносфери [302, 344, 345]. Због свега тога, развијање стратегија за ублажавање рањивости GNSS сигнала је од великог значаја. При томе, неопходно је да се на националном нивоу (Влада) примарно осигура одржавање безбедности, чак и у случају губитка GNSS сигнала, као и секундарно ублаже неповољни еколошки или економски утицаји. Фокус је на дефинисању критичних примена које захтевају заштиту, и одређивању нивоа ризика критичних примена (део 4).

Технике ублажавања RFI обухватају многобројне опције. Свакако, ефикасне технике за ублажавање ненамерног ометања, имају ограничени значај у спречавају намерних сметњи (ометање и спуфинг). Такође, избор технике зависи од врсте апликације, тј. степена потребне заштите. У ваздухопловству, технике ублажавања GPS рањивости често подразумевају употребу комплексних и скупих техника за ублажавање рањивости. Међу њима, избор адекватне, тј. оне која представља компромис између сложености, тачности, оперативне изводљивости и исплативости, од кључног је значаја. Такође, контруктивно/критичко поређење широког избора предлога, на основу општег критеријума примењивости (ефективност, реална примењивост, цена), значајно допуњава оно што недостаје у научној литератури.

О техникама ублажавања GNSS рањивости на ометање и спуфинг, детаљно је дато у ревијалним радовима [228, 288, 346] Технике ублажавања односе се на технике/методе, које омогућавају да прималац – мета напада, поврати своју способност адекватног/исправног позиционирања, неутралишући ефекат сметњи.



Слика 23. Поједностављени блок-дијаграм типичног SatNav пријемника (модификовано и преузето из [228])
AGC – *Automatic Gain Control*; PVT – *Position, Velocity, Time*

Укратко, **технике ублажавања** GNSS рањивости, генерално обухватају *front-end* технике, пре-корелационе (*pre-correlation*) и пост-корелационе (*post-correlation*) технике, као и навигационе технике (сл. 23). Потребно је нагласити да се због структурних разлика између сигнала ометања (*jamming signals*) и лажних сигнала (*spoofing signals*), за њихово ублажавање, користе потпуно другачији приступи – ометање се углавном превазилази коришћењем *front-end* и пре-корелационе технике, док се спуфинг ублажава пост-корелационим или навигационим техникама.

Front-end технике заснивају се на просторном филтрирању и обухватају технике *Switching Frequencies*[138], *Switching Antennas*[139] и *Adaptive Beamforming/Controlled Reception Pattern Antenna*, CRPA[140].

Пре-корелационе методе, као што су *Notch Filters, Pulse Blanking, Hilbert-Huang Transform, Short Time Fourier Transform, Spatial-temporal Adaptive Processing*, итд., укључују просторну, временску и спектралну обраду сигнала. У већини ових приступа, сигнал се трансформише у различите фреквенцијске домене у циљу процене одређене карактеристике интерферирајућег сигнала, или бољег раздвајања GNSS сигнала од интерферирајућег сигнала, као и издвајања компоненти трансформисаног домена, које представљају ометача. Процењени параметри често се користе за филтрирање ометача, док се издвојене компоненте користе за синтезу/реконструкцију, као и одузимање од мешаног долазног сигнала.

Пост-корелационе *(Link Level*) технике, обухватају *Successive Spoofing Cancellation, Subspace Projection Method* и *Integration* INS/GNSS. Ове технике укључују додавање других сензора, као и побољшану обраду сигнала. Технике су намењене за ублажавање спуфинга (не користе се за ублажавање ометања), јер се анти-спуфинг технике могу користити само уколико се аутентични сигнали могу раздвојити од лажних сигнала. GNSS аутентични сигнали могу се разликовати од фалсификованих, помоћу напредних техника обраде, као нпр. идентификовање вестигијалног (заосталог) сигнала, на основу мулти-корелационих ″банака″ података, а за навигацију користе само они, који су препознати као оригинални.

Навигационе технике, као што су *RAIM-Based Defences, Spatial Filtering* и *Navigation Level,* користе опсервабилне елементе, који су доступни на излазу већине фаза у праћењу пријемника, тако да није потребан *ad-hok* дизајн степена корелације пријемника, што последично омогућава примену на комерцијалне и одобрене пријемнике, а што је предност навигационе методе. Међутим, како је у фази навигације, ублажавање спуфинга једино могуће одбацивањем детектованих фалсификованих сигнала, недостатак методе је смањење доступности и континуитета навигационог решења.

Поменуте технике ублажавања GNSS рањивости на ометање и спуфинг, детаљно су анализирали *Morales-Ferre* и аутори [228]. Штавише, осим прегледа релевантне литературе и свеобухватне анализе главних концепата GNSS-а у последњих четрдесет година, ови аутори веома су садржајно, али и информативно

---

[138] Техника *Switching Frequencies* заснива се на употреби другог фреквенцијског опсега (фреквенцијске траке), када је примарни, изложен сметњама, и захтева употребу вишеканалног GNSS пријемника, у ситуацији у којој најмање један канал пријемника није изложен сметњама.

[139] *Switching Antennas* је техника, која се заснива на употреби већег броја антена и промени њиховог просторног распореда. Међутим, употреба већег броја антена/антенских низова које треба инсталирати у авиону и промена растојања између антена, ограничавају примену ове технике, нарочито за мале/некомерцијалне летелице.

[140] *Adaptive Beamforming/CRPA* је техника адаптирања формирања снопа, тј. контролише сноп зрачења GNSS антенског низа у циљу отклањања зрачења, које долази из правца ометача, и тако преосталу снагу сигнала усмери према GNSS сателитима. Ова прилагодљива просторна обрада (формирање снопа или нулто управљање) користи мулти-елемент антене, које су најчешће скупе и прикладније су за употребу у војне сврхе.

класификовали различите приступе за решавање и управљање сметњама, с фокусом на две главне претње, тј. ометање и лажирање. Поред тога, *Morales-Ferre* и аутори, на основу сопствених истраживања, која су била базирана на теоријској анализи, симулацијама и експерименту, закључују да не постоји техника, као ни комбинација техника, које би могла/е ублажити све врсте GNSS рањивости у погледу безбедности.

Ипак, у огромном спектру приступа, најпогоднија метода за детекцију сметњи у SatNav пријемнику, која се користи у ваздухопловству су AGC (део 5.2.1.1), TPD (*Time Power Detector*)[141] и FPD (*Frequency Power Detector*)[142] за детекцију ометања, као и SoS/D^3 *dual-antenna* детектор[143], за откривање спуфинга. Затим, за детекцију врсте ометања (*jamming* или *spoofing/meaconing*), неопходно је инкорпорирати два детекциона блока у SatNav пријемник, и то један у пре-корелационом домену (детекција ометача) и један на нивоу навигације (детекција спуфера). Имплементирање детектора ометача је релативно јефтино, док имплементирање пост-корелационог анти-спуфинг детектора захтева значајне модификације хардвера/фирмвера пријемника, због чега су они мање погодни за примену у области ваздухопловства.

Међу бројним алгоритмима за управљање сајбер безбедношћу, они који дају најбоље компромисе између сложености и перформанси за локализацију сметњи/налажење правца су *Angle of Arrival* (AoA)[144] алгоритми за ометање и лажирање; у циљу смањења додатне сложености/сметњи, због постављања додатних антена на авион, препоручују се највише три GNSS антене у авиону за локализацију сметњи засноване на AoA (једна антена за детекцију ометања, и две

---

[141]TPD (познат и као *Power Law Detector*, PLD, тј. детектор енергије); мери примљену енергија сигнала у временском домену (кратком временском интервалу); погодан је за бројне врсте ометача, међутим, мање је ефикасан за детекцију спуфинга, због упоредиве снаге аутентичног и лажираног сигнала [228 и овде цитиране референце].

[142] FPD, сличан је TPD детектору, али мери примљену енергију сигнала у фреквенцијксом домену [228 и овде цитиране референце].

[143] SoS (*Sum of Squares*) детектор (детектор збира квадрата), је *dual-antenna* детектор за убалажавање спуфинга. Користи математичке алате за оптимизацију полиномијалне функције методом збира квадрата (SoS), у циљу решавања проблема локализације сензорске мреже, проналажењем глобалног минимума кваратног полинома. Решавањем геометријског алгоритма, добијају се локазије појединачних сензора, користећи растојања између сензора. Наиме, измерена фазна разлика између пријемника и сигнала који долазе из истог правца, карактерише заједнички геометријски алгоритам. Израчунавањем двоструке разлике растојања између сателита, овај алгоритам се поништава, за лажне сигнале, док су за аутентичне сигнале геометријски алгоритми различити и не поништавају се при израчунавању двоструких разлика [228, 347]. На описаном принципу функционише и *Double Differences* (D^3) детектор. За детекцију спуфинга, користи се Monte Carlo симулација за добијање вероватноће појаве лажних аларма (брзина лажних аларма дефинисана је као број лажних идентикација спуфинга у односу на укупан број одлука током *Monte Carlo* симулационог теста [228]. D^3 детектор, у односу на SoS детектор је поузданији у сценарију *"mixed tracking"* [348].

[144] За одређивање локације ометача (пасивни извор који емитује непознат сигнал), не могу се користи апсолутна мерења, с обзиром на то да су референтна времена непозната. Због тога, за одређивање правца извора (ометача) користе се разлике, нпр. угла доласка (AoA) сигнала, где се AoA односи на мерења разлика фаза сигнала које емитују различите антене пријемника [228].

антене за детекцију спуфинга коришћењем *Sum of Squares*, SoS или D^3 детектора). Такође, у ваздухопловству, пре-корелациони приступи обухватају ANF (*Adaptive Notch Filters*)[145] и PBM (*Pulse Blanking Methods*)[146], као и MSTFT (*Modified Short Time Fourier Transform*)[147], а у зависности од тога да ли се користи, или не *a priori* интерференциони класификатор[148]. Ублажавање лажирања је ефикасно само у домену пост-корелације/навигације.

Еволутивни трендови SatNav у авионима, односно GNSS-у је развој двоструко/вишеструко фреквенцијских и мулти-констелационих пријемника, за побољшање тачности, доступности, континуитета и отпорности на RFI. Масовна производња савремених пријемника високе прецизности омогућава подршку за DFMC. У том контексту, ICAO и EUROCAE развијају регулативе, безбедносне захтеве и сертификације (од 2018. године), као и дефинишу стандарде (минималне оперативне перформансе) следеће генерације за DFMC. Међутим, овај тренд праћен је и изазовима у решавању RFI, као и неопходношћу обезбеђивања интегритета сложенијег *on-board* GNSS, безбедности рачунарских система и сл., јер је, за разлику од постојећих решења, потребно комбиновати много више информација из различитих извора/метода. У вези са детекцијом RFI и применом адекватних контра-мера у ваздухопловству, веома значајан је ICAO план (објављен 2017. године) за ублажавање GNSS RFI [350].

Побољшања, која се очекују од DFMC, укључујући и SBAS, као и ARAIM, подстичу фундаменталну промену улоге GNSS-а у области цивилног ваздухопловства, из допунског навигационог средства у примарни, док ће друга навигациона средства, ILS, VOR и DME, све више имати резервну улогу и користиће се у случају нефункционалности GNSS. Такође, *Free Route Airspace* (FRA), као нови концепт управљања ваздушним простором, којим ће авионима бити дозвољено да изаберу најекономичнију руту, као и променити перцепцију GNSS-а, од једноставног сензора до компоненте система управљања ваздушним саобраћајем, захтевајући проактивни приступ различитих заинтересованих страна, као нпр. пилота, контролора летења, авио-компанија, итд. [351]. Такође, у еволутивне концепте, који обухватају проминентну улогу GNSS-а спада и *Airbone Separation Assurance System* (ASAS) [315], као систем који асистира пилотима у

---

[145] *Notch Filters* (NFs), су *band-stop* филтери, који разлажу домен сигнала, тј. раздвајају сигнале из различитих домена; ови филтери елиминишу опсег, који карактерише уска *stop* трака. NFs за ублажавање интерференција, су типично дизајнирани као ANFs [228].

[146] PBM је најједноставнија техника, која се заснива на пригушивању импулса – сигнал се пригушује (постави на нулу) у периодима у којима је снага сигнала већа од одређене граничне вредности (прага) [228].

[147] MSTFT је модификација *Short Time Fourier Transform*, STFT методе (метода у којој се примењује Фуријеова трансформација малих, најчешће преклопљених временских сегмената сигнала). У MSTFT се за налажење и праћење пикова ометајућих сигнала, користи се NF бесконачног импулсног одзива за уклањање сигнала ометања. Овај приступ даје адаптивни и прецизнији временско-фреквенцијски приказ сигнала [349].

[148] Класификатор је део који разврстава улазне сигнале по класама, према одређеном правилу, а које се најчешће успоставља на основу бројних коректно означених примера за сваку класу; уколико су претходно познате карактеристике сигнала сметње (нпр. очекује се само одређена врста сигнала), онда је процена параметара добијена из сигнала добра, и довољна за разликовање сигнала [228].

одржавању потребног раздвајање између авиона, и даје информације о авио-саобраћају у околини. Тако ASAS доприноси повећању капацитета ваздушног простора, а с обзиром на то да авиони могу да лете на мањем међусобном растојању. Поред тога, ASAS не зависи од комуникација земља–ваздух.

Даљи трендови и изазови у сектору авијације, тј. авио-комуникацији, односе се на нпр. коришћење **5G мреже** (фуснота 25). Међутим, како су 5G сигнали базирани на електромагнетним (светлосним) таласима чије су таласне дужине реда величине милиметра, комуникациона решења заснована на коришћењу ове мреже, вероватно ће бити ограничена на дронове и авионе, који лете на малим висинама, као и у близини аеродрома. Поред тога, изазов је дизајнирање будућих 5G система, с адекватним положајем антене, а у циљу њиховог поузданог коришћење у авијацији.

У области ваздухопловства очекује се и примена ***Cloud-based* GNSS** пријемника (како се обрада GNSS сигнала не обавља у авиону, већ на земаљским серверима у *cloud*-у, стога може бити једноставније и прецизније од обраде сигнала у *on-board* GNSS пријемнику) [352], као и пораст примене техника машинског учења (за детекцију и класификацију ометања и спуфинга [353], детекцију јоносферских синтилација [354], итд.).

Поред изазова у вези са навигацијом заснованом на GNSS-u, постоје свакако и други, а који се односе нпр. на аспект комуникације [268, 355–357]. Тако на пример, *Wireless Avionics Intra-Communication* (WAIC) системи могу значајно побољшати оперативну ефикасност и флексибилност у односу на постојеће жичане системе у авиону [357]. WAIC је ограничен на апликације које се односе на безбедне, поуздане и ефикасне операције ваздухоплова, као што су мониторинг физичког стања авиона, инпута сензора, као и комуникација путем гласа, видеа или *fieldbus*-а [358]. Међутим, дизајн WAIC система не омогућава комуникацију за забаву током лета или с комерцијалним уређајима који се уносе у авион. Штавише, WAIC системи не подржавају никакве комуникације авион–земља, ваздухоплов–ваздухоплов и авион–сателит. Тако, корпорација *Gulfstream aerospace* је успешно завршила тест изводљивости концепта под називом *"Fly-by-Wireless"* система [359, 360].

Такође, одобрене релевантне иновације у ваздухопловној индустрији, које обухватају консолидоване технологије и нова достигнућа уведена у периоду од 2000–2019. године, дате су у ревијалном раду *Pereira* и аут. [361], у циљу сагледавања утицаја ових иновација на индустрију, генерално, кроз веома корисну класификацију остварених постигнућа за сектор ваздухопловства у пет кластера иновација, и то: (1) авио-технологија (додатне вредности у вези с ефикасношћу и одрживости; (2) иновације у путничким услугама, персонализованијим услугама и побољшању корисничког искуства; (3) иновација у летењу (додатне вредности у вези с безбедношћу и безбедним окружењем; (4) пословно и оперативно управљање, побољшање процедура и прихода; (5) опште примене (додатне

вредности у вези са ваздухопловством[149] 4.0, тј. повећањем аутоматизације и размене података, укључујући сајбер-физичке системе, IoT и *cloud* рачунарство).

5.3. ПРИМЕНА ФАЗИ ЛОГИКЕ ЗА АНАЛИЗУ ПАРАМЕТАРА

За решавање различитих, сложених проблема у пракси, пројектују се различити и све софистициранији алгоритми машинског учења, као што је модел дубоког учења (*Deep Neural Network*). Тако, интерпретабилно[150] машинско учење, омогућава генерисање човеку разумљивих модела, као што су фази логички модели [363]. Данас се користе различите технике машинског учења, као то су фази логика, неуронске мреже, SVM (*Support Vector Machine*), као и хибридне технике.

Фази логика, као метода вештачке интелигенције, омогућава генерисање нових модела и избор бољих решења у многим процесима. Основна карактеристика методе је њена универзалност – метода се може користити у свим областима моделовања и оптимизације и најсложенијих процеса. Поред тога, предности фази концепта су базираност на лингвистичким варијаблама, једноставност, флексибилност, толерантност на непрецизност података, могућност моделовања нелинеарних функција, итд.

Различите апликације у којима фази логика има значајну улогу су: управљање (индустријске апликације), закључивање (транспорт, екологија, интелигентни системи, итд.), препознавање узорка (анализа слике, процесирање звука и сигнала) и квантитативна анализа (статистика, менаџмент), тј. подручја примене: транспорт (контрола саобраћаја, хеликоптери, подземне железнице, итд.), роботи, индустрија, инжењеринг, медицина, итд.

Генерално, теорија фази логике у данашње време, доживљава велику експанизију у различитум научним областима, нарочито техничким, тј. у сложеним системима где постоји неизвесност, која се односи на улазне податке неопходне за доношење одређених одлука. Управо такви системи су навигациони (нпр. GPS), као и системи за надзор (ADS–B).

Ово поглавље садржи кратки опис основних појмова у вези са фази логиком (дефиниција фази скупова, основне врсте функција припадности на основу којих се врши класификација скупова, анализа фази система закључивања, методе закључивања, предности и разлике, као и методе дефазификације (део 5.3.1), као и

[149] Сада смо у добу 4. индустријске револуције, назване Индустрија 4.0., тј. новој ери иновација у технологији, посебно у технологији базираној на вештачкој интелигенцији (AI). Након што су интернет и мобилни интернет обележили 3. индустријску револуцију, AI технологије, подржане подацима, стварају свет Индустрије 4.0. – ″израз који се користи за описивање садашњег тренда аутоматизације индустријске технологије и размене података, који укључује сајбер-физичке системе, IoT, *cloud* и когнитивно рачунарство, као и развој паметне фабрике″ [195].

[150] Интерпретабилност, тј. разумљивост понашања, представља способност описа понашања реалног система/модела на разумљив начин (разумевање начина интеракције параметара модела, тј. података, који су подаци важни и које релације постоје међу њима) [362].

имплементацију фази-логичких алгоритама за класификовање GPS сигнала (део 5.3.2).

5.3.1. Фази логика – основе концепције

Теорија фази логике развијена је (Лофти Задех, 1965. године) [364] у циљу превазилажења проблема у вези с доношењем одлука у сложеним процесима, који садрже велики број разнородних података и информација, и нарочито недовољни број информација, од којих неке могу бити и непоуздане [365, 366]. Фази логичко моделовање омогућава руковање исказима (описаних људским језиком) и њихово конвертовање у рачунарске алгоритме погодне за обраду на рачунару.

Фази логика заснива се на теорији скупова (″расплинути″ или ″неразговетни″ скупови), који представљају адекватан математички алат за третирање неизвесности, субјективности, вишезначности и неодређености. Представља проширење конвенционалне логике – то је вредносна логика, која комплексне појаве из реалности описује једноставним фази скуповима[151] (скуп којем елементи могу припадати с различитим степеном припадности).

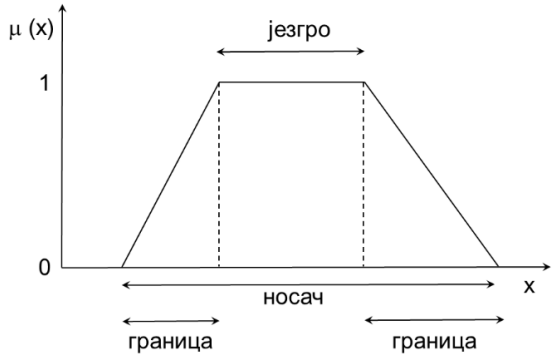
Суштина **фази приступа** је проширивање класичне теорије скупова (према којој неки елемент скупа *x* из посматраног универзалног скупа *X* припада или не припада конкретном скупу А), дефинисањем парцијалне припадности. У теорији фази скупова, карактеристична **функција припадности** (*membership function*)[152] генерализована је функцијом припадности, μ_A тако да сваком елементу из универзалног скупа придружује вредности из интервала [0,1].

Фази скуп А, представља се скупом парова: $A=\{(x, \mu_A(x)), x \in X\}$, где је $\mu_A(x)$, степен припадности елемента *x*, скупу А. **Особине** фази скупова су висина (највећи степен припадности фази скупа), носач (класичан скуп елемената $x \in X$, $\mu_A(x) > 0$) и језгро (центар, који је подскуп универзалног скупа X, а који садржи све елементе са степеном припадности 1) (сл. 24). Фази скуп А чији се носач састоји само из једног елемента универзалног скупа, за који је $\mu_A(x) = 1$, назива се фази синглтон (*fuzzy singleton*). Фази број је нормализован и конвексан фази скуп чије језгро садржи само једну тачку. Елемент $x \in X$, за који је $\mu_A(x) = 0{,}5$, назива се тачка проласка (*crossover point*). Логичке операције над фази скуповима су специјално дефинисане операције, као што су операције уније, пресека и комплемента фази скупова. Ове операције изведене су преко фази оператора (T-норма и S-норма). У екстремним случајевима, када је $\mu_A(x) = 1$, или 0, што значи да *x* припада или не припада А, тако да се фази скуп своди на *crisp* (класичан) скуп са Буловом функцијом припадности.

---

[151] Операције пресека, уније и комплемента у *crisp* (″оштра″) логици, у *fuzy* логици кореспондирају изразима/везницима *and*, *or* и *not*, тако да се помоћу њих могу градити сложенија тврђења.

[152] Функција припадности представља криву, која дефинише пресликавање тачака (појединачних мерења) из улазног вектора у припадајућу вредност из интервала од 0 до 1.



Слика 24. Основне карактеристике фази скупова (граница, носач и језгро)

У зависности од функције припадности, $\mu_A(x)$, фази скупови могу бити нормализовани (функције припадности бар једног елемента универзалног скупа има вредност 1) или субнормализовани (функције припадности има припадну вредност мању од 1). Најчешће врсте **функција припадности**[153] су: троугаона, трапезоидна (сл. 25а и б), праволинијска, Гаусова, итд. Тако нпр., троугаона функција припадности дефинисана је на следећи начин (сл. 25.а):

$$\mu_{(x)}=\begin{cases} 0, \text{ за } x < a \\ \frac{x-a}{c-a}, \text{ за } a \le x < c \\ \frac{e-x}{e-c}, \text{ за } c \le x < e \\ 0, \text{ за } x > e \end{cases} \tag{4}$$

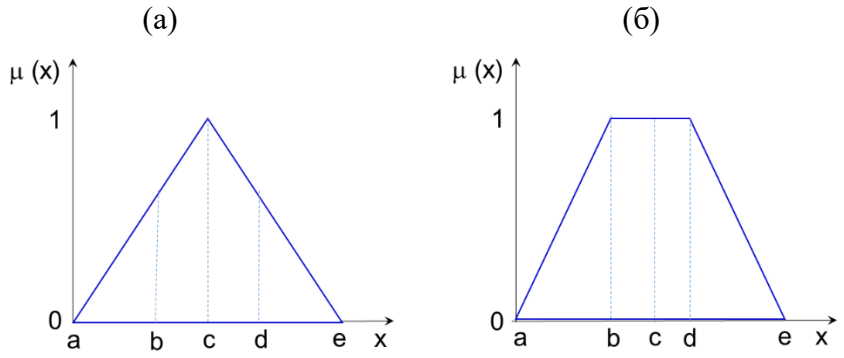
док је трапезоидна дефинисана са (сл. 25.б):

$$\mu_{(x)}=\begin{cases} 0, \text{ за } x < a \\ \frac{x-a}{b-a}, \text{ за } a \le x < b \\ 1, \text{ за } b \le x < d \\ \frac{e-x}{e-d}, \text{ за } d \le x < e \\ 0, \text{ за } x > e \end{cases} \tag{5}$$

Фази системи закључивања захтевају да, осим дефинисане функције припадности појединих лингвистичких променљивих, буду дефинисана и **правила закључивања**. **Фази систем закључивања** (*Fuzzy Inference System*) јесте најзначајнији алат за моделовање – основна структура *Fuzzy Inference System* је модел, који пресликава улазне карактеристике у улазне функције припадности, улазне функције припадности у правила, правила у скуп излазних карактеристика,

[153] Избор облика функције припадности зависи од специфичности система који се анализира (погодности), брзине, ефикасности, итд; трапезоидне и троугаоне су погодне за операције у реалном времену, јер су једноставне за анализу и омогућавају добијање резултата прихватљиве тачности.

излазне карактеристике у излазне функције припадности, а излазне функције припадности у јединичну вредност излаза, односно одлуку у складу са излазом.



Слика 25. Графички приказ фази фунција припадности: троугаона (а) и трапезоидна (б)

Лингвистичка променљива је променљива чији су аргументи фази бројеви (нормални и конвексни) или је уопштено представљена фази скупом. Одређена је лингвистичким вредностима, које су дефинисане функцијама припадности (начином на који неки елемент универзалног скупа пресликава/мапира у интервал [0,1]). Лингвистичка променљива је четворка (x, A(x), U, M), где је x – назив лингвистичке променљиве, A(x) – скуп лингвистичких вредности (термина, израза), које може пропримити лингвистичка променљива x, U – стварни физички домен у коме елементи из скупа A добијају нумеричке вредности (континуирана или дискретна) и M – семантичка функција која даје квантитативно значење лингвистичким изразима; то је функција која сваком x из A, придружује фази подскуп од U.

Основа за добијање фази излаза, су фази правила (заснована на IF–THEN, тј. **АКО–ОНДА**). Фази правила АКО–ОНДА, су математичка правила у облику: АКО је x = A, ОНДА је y = B (x и y су лингвистичке променљиве, док су A и B лингвистичке вредности на универзалним скуповима X и Y); део правила ″x је A″ назива се антецедент (претходник, премиса или претпоставка), док се ″y је B″ назива консеквенца (последица или закључак). Максималан број правила одређен је бројем улазних величина, као и бројем лингвистичких вредности[154]. Процес добијања свеобухватног закључка од појединачних премиса из сваког од правила, назива се агрегација правила, која даје компактну математичку представу целокупне базе знања. Агрегација се своди на неку од основних логичких операција (коњукцију или дисјункцију, односно, T-норму или S-норму).

Дакле, фази правило описује узрочно-последичне везе између улазних и излазних променљивих; с аспекта аутоматизације, представља спрегу сензорских

[154] Максималан број правила одређен је бројем улазних величина и лингвистичких вредности. Ако је број улаза n, а број вредности за сваку појединачну величину m, онда је максималан број правила m^n (за све могуће комбинације). Ако број улаза није превелик, табеларни приказ је погодан начин представљања свих случајева.

информација и управљачких акција. Бинарном фази релацијом (R), сваком пару променљивих (x и y) из Картезијевог производа придружује се вредност $\mu_R(x,y)$, тј. вредност функције припадности. Фази закључивање је процес трансформације фази улаза у фази излаз[155], коришћењем фази логике. АКО–ОНДА је фази релација, која се назива импликациона релација (даје функционалну везу између премисе и последице правила). Постоје бројне импликационе релације, тј. импликациони оператори, који фази правилима дају значење, као што су Мамдани импликација (импликација типа минимума), импликација типа производ, Задехова импликација (максимум-минимум импликациони оператор), итд. Процесом агрегације, представља процес формирања закључка на основу појединачних закључака добијених сваким од појединачних правила. Тако, основни функционални елементи фази система закључивања су:

- фазификација[156] (*fuzzifier*) – трансформише реалне променљиве у фази променљиве
- база знања (базе података и правила)
- функција припадности (*membership functions*, MF) базе податак – дефинише вредности променљивих које се користе у фази правилима
- систем закључивања (*inference engine*) – обрађује фази АКО–ОНДА (*if–then*) правила и дата ограничења у циљу генерисања коначних излаза/закључака; карактерише га нелинеарно мапирање простора улазних променљивих у простор излазне променљиве
- дефазификација[157] (*defuzzifier*) – трансформише фази променљиве у реалне променљиве.

Постоје различите фази методологије, тј. системи фази закључивања (*Fuzzy Inference System*), као нпр. Мамдани фази метода закључивања [367] и Такаги-Сугено-Кангов (TSK) фази метод [368, 369]. Основна разлика између ова два алгоритма фази логике је то што се у Мамдани моделу дефазификују излази фази скупова, док су у TSK моделу, излазне функције припадности линеарне функције, или су константе. Тако, Мамдани фази правила називају се фази правила нултог реда, док се TSK фази правила, називају фази правилима првог реда. У односу на Мамдани *Fuzzy Inference System*, TSK модел је рачунарски ефикаснији и нумерички тачнији модел [370]. У циљу повећања тачности и разумљивости понашања, предложена је и комбинација Мамдани модела и TSK, као основа неуро-фази

[155] Улазне вредности су најчешће представљене бројем (квантитативно) и жели се да се и излазне вредности представе на такав начин. Међутим, у фази систему, анализирани систем је описан квалитативно (вербално) преко предикционих правила. Због тога, бројчане вредности морају се конвертовати на одређени начин, тј. фазификовати (конвертовање сваког бројног улазног податка у степен припадности, који је различит за свако правило). Фазификоване вредности се обрађују са АКО-ОНДА, у складу са скупом унапред дефинисаних правила базираних на знању експерата из одређене области. Као резултат, добијају се излазни фази скупови. Из сета ових излазних скупова, применом правила, дезификатор, прерачунава излазне тачне вредности, тј. контролне акције које треба предузети.

[156] Назив за фазификацију је и кодирање.

[157] Назив за дефазификацију је и декодирање.

мрежне архитектуре, тј. веома робустног модела (захваљујући инкрементном учењу адаптира се на променљиве карактеристике проблема током времена) [371].

Мамдани модел састоји се од следећих корака: 1. Дефинисање скупа фази правила; 2. Фазификација улаза (коришћењем улазних функција припадности); 3. Примена фази оператера (комбиновање фазификованих улаза према фази правилима у циљу утврђивања снаге правила); 4. Примена методе импликације (налажење последица правила кобиновањем снаге правила и излазне функције припадности); 5. Агрегација излаза (комбиновање последица у циљу добијања излазне расподеле); 6. Дефазификација излаза (процес превођења резултата, који су у облику фази скупа, у бројне вредности, коришћењем различитих метода, као нпр. методе тежишта и метода максималне припадности).

Такаги-Сугено-Канг (TSK) фази логички модел омогућава описивање сложених, високо нелинеарних модела, и то, коришћењем малог броја правила [372–374]. Међутим, овај модел карактерише мања разумљивост презентације знања. Основа TSK модела заснива се на чињеници да одређени сложени систем представља комбинацију међусобно повезаних подсистема, представљених са K региона у посматраном простору знања. Понашање система у појединим регионима, може се описати једноставним функционалним зависностима. Уколико су ове зависности линеарне, и уколико се сваком региону додели по једно правило, онда се TSK фази-логички модел може представити са K правила:

R_i: АКО x_1 је A_{i1}, x_2 је A_{i2}... и x_n је A_{in}

ОНДА: $y_i = a_i x_i + b_i$ (i = 1, 2, 3,..., K)

где су: R_i је i-то правило; x_1, x_2,... x_n су улазне варијабле; A_{i1}, A_{i2}, ..., A_{in} су фази скупови додељени одговарајућим улазним променљивим; y_i је вредност излазног i-тог правила; a_i и b_i су параметри последичне функције. Коначан излаз TSK фази-логичког модела за произвољни x_k улаз, рачуна се из израза:

$$\hat{y}_K = \frac{\sum_{i=1}^{K} \left[\beta_i(x_k) y_i(x_k)\right]}{\sum_{i=1}^{K} \beta_i(x_k)}, k = 1, 2, 3, \ldots, \mathrm{N} \tag{6}$$

где β_i представља ниво аквизиције (*firing strength*) *i*-тог правила,

Израз (6) се може приказати у облику:

$$w_{ik} = \frac{\beta_i\,(x_k)}{\sum_{j=1}^{K} \beta_j(x_k)}, k = 1, 2, 3, \ldots, \mathrm{N} \tag{7}$$

где је w_{ik} нормализовани степен аквизиције *i*-тог pravila за *k*-ти узорак.

TSK процедура, разликује се од Мамдани, у процесу прикупљања и дефазификације. TSK обрада правила/фази закључивања користи "*min-max*" технику закључивања за израчунавање закључака (нумеричких) из правила, а на основу вредности улазне променљиве у систем. Различита правила могу имати различиту јачину, тј. различит степен истинитости, дајући различите резултате. Обрада правила, заснива се на одређивању истинитосне вредности правила, тј. минималне вредности узорка у правилу. Ова вредност правила примењује се на последице у правилу. Уколико се један фази излаз добије применом више

различитих фази правила, онда се тај фази излаз поставља на максимално добијену вредност. Резултат обраде правила, тј. "*min-max*" одлучивања је комплетан скуп вредности фази излаза, који представљају утицај свих правила, чија је истинитосна вредност већа од 0.

За генерисање алгоритма TSK фази-логичког модела, може се комбиновати груписање улазних података неком методом кластер анализе, затим подешавања параметара методом најмањих квадрата, као и WRLS (*weighted recursive least-squares*) процедуром [372–374]. С обзиром на карактеристике TSK модела (брзо израчунавање, коришћење линеарне технике, једноставна математичка анализа и сл.), овај фази-логички систем користи се када је потребан брз одзив система, односно када систем мора радити у реалном времену.

Теорија фази логике примењује се, у различитим областима, као што су техника, технологија, саобраћај, медицина, економија, менаџмент, итд. [375–383], а у авио-сектору *Fuzzy Logic Controller* (FLC)[158] обухвата контролу GPS-а и сателита, навигацију беспилотних летилица, ауто-пилоте, итд. Најскорије, поред фази логике, која се бави различитим аспектима представљања и процесирања непоузданих информација, омогућавајући апроксимативно резоновање у области система заснованих на знању, развијена је и техника неуронских мрежа, ефикасна рачунарска дисциплина, која обезбеђује обучавање и адаптацију на бази примера [384]. С обзиром на карактеристике (предности и недостатке), сваке од техника, фази логика и неуронске мреже се допуњују – фази системима недостаје аспект обучавања, адаптирања и паралелног процесирања, што обезбеђују неуро мреже, док неуро мрежама недостаје људска интеракција/презентација знања, што су добре особине фази логике. У том смислу, добијање ефикасне хибридне технике, тј. фази-неуро система, садашњи је тренд истраживања у овој области [385, 386]; област се интензивно развија, нудећи бројна, принципијелно нова решења. Неки од хибридних система су фази-неуро мреже[159], кооперативни неуро-фази системи[160], хибридни неуро-фази системи[161], итд.

---

[158] FLC – фази логични контролер користи фази логику и лингвистичке системе за опис система којим се управља.

[159] У фази-неуро мрежама, фази методе се користе за побољшање метода обучавања и перформанси неуро мрежа, тако што се нпр. користе фази правила за промену брзине учења, пројектовањем неуро-мрежа, које садрже фази улазе и сл.

[160] У кооперативном неуро-фази систему, неуро мрежа се користи за побољшање фази методе, тј. за подешавање параметара основног фази система (подешавање функција припадности, фази правила, тежинских коефицијената правила и сл.).

[161] Хибридни неуро-фази системи су савремени системи у којима се неуро-мреже и фази системи комбинују тако да дају хомогену структуру – специфична неуро-мрежа с фази параметрима, или фази систем имплементиран у паралелном дистрибуираном облику. Примери ових система су [384] ANFIS (*Adaptive Neuro-Fuzzy Inference System*) [387], GARIC (*Generalized Approximate Reasoning-based Intelligent Contro*l) [388], NEFCON (*NEuro-Fuzzy CONtrol*) [389], итд.

5.3.1.1. Фази логички алгоритми за класификовање GPS сигнала – кратки преглед литературе

Теорија фази скупова, континуирано привлачи пажњу бројних истраживача из различитих научних области. Примена фази-логичних и, нарочито фази-неуро техника, је у порасту, а у области авијације, ови системи користе се за решавање различитих проблема у вези са навигацијом, тј. проблемом губитка GPS сигнала.

Већина савремених система за навигацију зависи од GPS-а. Међутим, *Multipath* ефекат (настао као резултат *Line Of Sight*, LOS, као и рефлектованих сигнала) и *Non-Line-Of-Sight* (NLOS), или индиректног пријема GPS сигнала, доводи до погоршања перформанси GPS-а, нарочито у урбаним срединама. С друге стране, навигациони системи, посебно *Inertial Navigation Systems* (INSs), су важне компоненте у различитим цивилним/војним применама. GPS и INS имају широк спектар навигационих функција, а сваки од ових система, појединачно, има одређене снаге и слабости [390]. Тако, тачност INS се смањује с временом, због чега је потребно периодично ажурирање система коришћењем екстерних мерења. У том циљу, INS мерења интегришу се с GPS мерењима, резултирајући навигационим системом супериорних перформанси у поређењу са индивидуалним GPS или INS системом.

Због поменутих слабости GNSS система, од намерног ометање и спуфинга, до губитка тачности података у урбаним срединама (лош *geometrical-dilution-of-precision* коефицијент, вишеструких рефлексија, као и шума у GPS сигналима, што захтева коришћење филтера уског пропусног опсега), неопходни су нови концепти интеграције GNSS система – GNSS систем није аутономан, тако да је овај тип навигационог система погодан за интеграцију с другим система, у циљу остваривања веће аутономије.

Један од начина превазилажења проблема нестанка GPS сигнала, је ANFIS техника (фуснота 161). Као што је поменуто, ANFIS је метода машинског учења, која користи комбинацију неуронске мреже и фази логике за добијање поузданијих излазних података, у односу на различите инпуте (променљиве). Примењује се у различитим областима, као што су медицина [391], хидрологија [392], обновљиви извори енергије [393], навигација [394, 395], авио-саобраћај [396], итд.

Тако, у раду *Hiliuta*-а и аут. [397] описан је нови концепт у вези с интеграцијом GNSS система и INS-а, заснован на вештачкој интелигенција, која се базира на примени фази логике, тј. на ANFIS-у. Подаци GPS-а (референтни навигациони систем) и INS-а, користе се за изградњу структуриране базе знања, као и за предложен фази систем, који је обучен да даје кориговане навигационе податке. У недостатку GPS информација, систем функционише на основу података из INS-а, користећи алгоритам фузи корекције. Као што су *Hiliuta*-а и аут. [397] показали, тачност обученог ANFIS-а, под одређеним условима, а у недостатку података из референтног навигационог система, је боља него тачност самосталних INS-а.

За превазилажење проблема нестанка GPS сигнала у раду [398] предложена је и варијанта ANFIS технике, односно *Dynamic Adaptive Neuro-Fuzzy Inference System* (DANFIS). Ова техника користи се за предвиђање INS грешке, током прекида GPS-а на основу тренутних (претходног необрађених) INS података. Добијени резултати

показују супериорност технике у односу на Калманово филтрирање и конвенционалне ANFIS методе.

Такође, *Sun* и аут. [399], применили су нове алгоритме базиране на ANFIS техници, за класификовање GPS сигнала, користећи познате репрезентативне променљиве из ″сирових″ GPS мерења (јачина примљеног сигнала, временска разлика јачине примљеног сигнала, хоризонтално и вертикално *Dilution Of Precision*, угао елевације сателита и угао азимута, резидуални псеудодомет, конзистентност између промене псеудо-домета и брзине псеудо-домета, као и број видљивих сателити). Дизајнирани алгоритам заснован на ANFIS не захтева додатне трошкове хардвера, а класификовање GPS сигнала засновано на већем броју улазних променљивих, обезбеђује робустни метод класификовања GPS сигнала, и флексибилнији је од приступа класификовања GPS сигнала, заснованог на једној променљивој. Дизајнирање алгоритма састоји се у следећем: креирању *offline* скупа података (бројни LOS, *multipath* и NLOS подаци)[162], примени PCA на GPS улазне променљиве (PCA се користи за претходну обраду података у циљу издвојања кључних карактеристика, смањења димензија система и, поједностављивање правила за следећи корак, тј. примену ANFIS-а), затим, обуци заснованој на ANFIS-у (примењеној на репрезентативном скупу података), у циљу добијања обучених правила и класификацију согнала (LOS, *multipath* и NLOS података) *Fuzzy Inference System*-а. Како *Sun* и аут. истичу, у односу на друге класификаторе GPS сигнала, као што је нпр. однос сигнала и шума (*signal to noise ratio*), предложени алгоритам даје већу тачност за инпут податке прикупљене са исте локације. Међутим, тестирање ANFIS модела за скупове података који нису прикупљени с исте локације, показала је да промена окружења деградира перформансе алгоритма, указујући на осетљивост алгоритма на такве проблеме.

За аутономност и практичну употребу UAS, од суштинског значаја је прецизна процена позиције и оријентације, у чему се UAS најчешће ослања на GPS и INS. Због чињеница да GPS може бити недоступан (у близини препрека) или ометан (намерно), тако да када GPS и INS нису у могућности да предвиде и коригују UAS позицију, FLS помаже да се аутономно предвиди тачан положај и оријентација UAS, односно навигацији. У раду [379], аутори су дизајнирали и имплементирали *Fuzzy Inference System* заснован на три модуларна FLS, и то: *Latitude-Longitude* FLC, *Altitude* FLC и *Heading* FLC за предикцију положаја UAS и помоћ у аутономној навигациији UAS. У односу на конвенционалне контролере[163], FLS је прилагодљивији, обухвата шири спектар радних услова, као и јефтинији за развој.

---

[162] *Multipath* ефекат (настао као резултат *Line Of Sight*, LOS, и рефлектованих сигнала) и *Non-Line-Of-Sight*, NLOS, или индиректног пријема GPS сигнала, доводи до погоршања перформанси GPS-а, нарочито у урбаним окружењима.

[163] *Proportional integral derivative* (PID) контрола – универзално прихваћен алгоритам управљања [400], робустних перформанси и функционо једноставна. PID користи разлику (грешку) између референтне/жељене вредности контролисане променљиве и њене измерене вредности, у циљу добијања оптималног одговора у жељеном опсегу. PID алгоритам (обрада грешке), састоји се од следећих коефицијента: пропорционалног (обрада тренутне вредности грешке), интегралног (интегрише или рачуна збир грешака у протеклом временском прозору) и деривативног (брзина промене грешке између последња два читања), који се мењају за добијање оптималног одговора.

Такође, у раду [401], разматра се интеграција UAS-а у NAS, тј. алгоритам фази логике за безбедно и ефикасно аутоматизовање арбитраже у ваздушном саобраћају, на основу улазног сигнала, које добијају земаљске АТС станице из авиона, као и излазног сигнала од АТС земаљских станица до авиона. Фази логика се користи за проналажење најбољег решења, које обезбеђује план безбедног распореда авиона (с посадом или без посаде).

У авио-сектору, *Fuzzy Inference System* коришћен је као надзорни експертски систем, за анализу перформанси авиона при слетању [378]. Конкретно, коришћен је Мамдани модел, којим су фазификоване четири улазне променљиве (Максимална тежина при слетању, Брзина прилаза, Нападни угао и Висина одлуке), према утврђеној бази фази правила, затим, добијене су излазне функције припадности и израчуната јединствена дискретна вредност (методом дефазификације). Показало се да је ова анализа ефикасности симулације слетања авиона, у доброј сагласности с реалном ситуацијом [402].

На крају, предложене су различите методе машинског учења и фази логике у изазовима идентификовања и категоризације великих количина података о летовима авиона, захваљујући доступношћу ADS–B транспондера у комерцијалним авионима, као и порастом броја земаљских станица које обезбеђују јавни приступ њиховим подацима. Ове велике количине података о авио-саобраћају могу бити од користи у широком спектру АТМ анализа које се ослањају на оперативне податке и статистику [403].

6. ADS–B АВИО СИСТЕМ: АРХИТЕКТУРА И САЈБЕР БЕЗБЕДНОСТ

> *"У цивилном ваздухопловству, револуција је у току – и она нема никакве везе с новим моторима, суперсоником, ултра-дугим летовима или in-flight Wi-Fi. Оно што ће уштедети време, гориво и животе људи је невидљиво повезивање постојећих технологија у систем управљања ваздушним саобраћајем прилагођен 21. веку."* [404]

Убрзо након *Charles Lindbergh*-овог (сл. 26) лета преко Атлантика (1927)[164], авијација је постала глобална индустрија. Кључни покретач развоја цивилног ваздухопловства је потреба за брзим транспортом људи и робе, а константно смањење реалних трошкова путовања авионом, довело је до тога да ова путовање не представљају луксуз, и да постају приступачнија све већем броју људи [406, 407]. Очекује се да ће до 2034. године, у односу на 2016. годину, ваздушни путнички и теретни саобраћај, бити двоструко повећан. Због енормног пораста броја прелета, неопходно је унапређење коришћења ваздушног простора, што се превенствено односи на економичност и брзину, без угрожавања безбедности.

Очекивано повећање броја летова неминовно ће довести до преоптерећености ваздушног простора, као и до повећаног оптерећења и стреса контролора летења и пилота, који осигуравају безбедно, поуздано и ефикасно путовање авионом. Широка употреба беспилотних летелица (UAS)/дронова додатно ће повећати гужву на небу у блиској будућности, где ће милиони дронова коегзистирати са авионима с посадом [228]. Због тога, неопходно је омогућити нова техничко-технолошка решења, као и нову опрему у свим сегментима, како у оквиру земаљске инфраструктуре, тако и у ваздухопловима (*on-board*) за постизање квалитетнијег надзора и обраде података.

У циљу ефикасног решавања различитих питања у вези са капацитетом ваздушног простора, FAA и EUROCONTROL уводе следећу генерацију ваздушног транспортног система NextGen [7] и SESAR [8] програме у циљу модернизације ATM-а и побољшања слања/пријема дигиталних информација. Ово представља еволуцију земаљске ATC, у ону засновану на сателитским контролним системима с бројним комуникационим везама и услугама. Поред тога, у циљу увођења јединствених стандарда у ваздухопловству, ICAO подржава имплементацију сличних програма широм света.

---

[164] Пре него што је *Charles Lindbergh* (1902–1974) направио први лет преко Атлантског океана [405], већина Американаца, сматрала је да је путовати авион веома рискантно. Међутим, након што је Линдберг безбедно слетео у Париз, након 33 h 30 min лета од *Long Island*-а (*New York*), Американци су стекли поверење у ову врсту путовања. Тако, далеке 1929. године, више од 170.000 путника укрцало се у авионе у USA (скоро три пута више од броја путника претходне године). Након свог трансатлантског лета, Линдберг је искористио популарност за промоцију развоја авијације, а заједно са својом супругом *Anne Morrow Lindbergh*, која му је била копилот и навигатор, Линдберг је уцртао међународне ваздушне руте за нове комерцијалне авио-компаније које су летеле преко Канаде до Азије (1931). Две године касније, Линдбергови су прелетели 30.000 миља мапирајући комерцијалне руте преко Атлантика. Остало је историја...

Слика 26. *Charles Lindbergh* са супругом *Anne Morrow Lindbergh* (1932) (преузето из [408])

Због неопходности модернизације ATM-а, покренута су два пројекта (2004), и то, FAA пројект *NextGen* и Eurocontrol CASCADE програм. Ови пројекти би требало да обезбеде развој *Automatic Dependent Surveillance – Broadcast* (ADS–B) и потпуну интеграцију овог прецизног система за надзор, у циљу смањења зависности авио-система од скупе и застареле радарске опреме [409]. ADS–B-у је додељен посебан ASTERIX (*All Purpose Structured Eurocontrol Surveillance Information Exchange*) протокол категорије 21, за размену информација у ваздухопловству [410].

FAA је 2010. године објавила финалну одлуку, која се односи на амерички национални ваздушни простор, захтевајући да сви авиони (одређене класе) буду опремљени ADS–B-ом (ADS–B Out) до 1. јануара 2020. године [411]. Уз незнатна временска померања, услед новонастале пандемије болести корона вируса изазване вирусом SARS-CoV-2 у 2019 (Covid-19), између осталих фактора, 2022. година означена је као крај временског оквира за имплементацију ADS–B система (ADS–B је сада обавезан у Америци, Аустралији и Европи) као глобалног стандарда у комерцијалном ваздухопловству, а који представља гигантски корак у модернизацији и повећању квалитета ваздухопловних операција.

Који су изазови ове модернизације? Као што се истиче у FAA документу [412], примена ADS–B не доводи до пораста безбедносног ризика по авио-системе. Бројни су бенефити које ADS–B систем нуди и ATC-у, и пилотима, као што је значајни пораст *situational awareness* летачке посаде (омогућава доношење пилотских одлука уз пуну свесност о утицају на друге кориснике) и ефикаснију оперативност контролора (квалитетнија координација и безбедно одвијање ваздушног саобраћаја на основу информација о ваздухопловима у реалном времену). Затим, у односу на традиционалне радарске системе, ADS–B смањује

трошкове постављања и одржавања система, значајно повећавајући покривеност подручја.

ADS–B трансформише све сегменте авијације. Прецизност у реалном времену, заједничка свест о ситуацији, као и напредне апликације (за пилоте, као и контролоре), које повећавају безбедност и ефикасност у ваздуху, као и на полетно-слетним стазама (пистама), смањујући трошкове и штетне утицаје на животну средину, суштинске су карактеристике ADS–B надзора.

Дакле, предности ADS–B могу се сажети у следећим чињеницама [412]:

- ADS–B у реалном времену, данас је преферирани метод надзора за ATC
- коришћење ADS–B услуга авио саобраћаја, метеоролошких услова и информација о лету, повећава безбедност генералне авијације
- коришћење напредних ADS–B апликација, повећава безбедност, као и ефикасност.

Међутим, ADS–B има одређене слабости, узроковане недостатком интегритета или аутентичности у емитованим текстуалним порукама, а које могу бити изложене различитим сметњама, коришћењем SDR (фуснота 136) и комерцијално доступне опреме. Дакле, ADS–B има веома једноставан *"free to air"* протокол који је рањив на различите сајбер-физичке нападе. Питања која следе су: Да ли је отворена критика и бављење овом темом тривијално, као и која су решења? Постоје ли начини да се елиминишу ове сајбер претње?

Ова питања, отварају нека нова, али, били спремни или не, ADS–B је стигао. Због чега је, две године након ступања на снагу поменуте мандатне уредбе, систем ADS–B и даље тема, да ли су идентификовани проблеми и који су најновији изазови и могућности? Шта треба очекивати, и да ли ADS–B нуди бенефите авио-компанијама након мандата? Да ли су пилоти и контролори летења, као крајњи корисници, довољно укључени и едуковани о свим аспектима функционисања ADS–B система, а посебно да ли су упознати с могућим безбедносним изазовима, тј. ометањима, којима могу бити изложени, као и адекватним против-мерама?

Да бисмо почели, као и добили неке одговоре, неопходно је разумевање ове нове технологије. Основе ADS–B (технологија, тј. инфраструктура, комуникациони протоколи и ADS–B подаци, имплементација и ефикасност) дате су у поглављу 6.1, као помоћ за разумевање безбедносних проблема и ограничења протокола, као и за сагледавање различитих начина на које ADS–B може бити потенцијално нападнут (поглавље 6.2), и последично угрозити безбедност ваздухопловства у свим његовим аспектима. Како ADS–B опрема може имати различите интерфејсе с пилотима (од једноставног, до управљачког интерфејса с напредним карактеристикама), разматрају се неки аспекти односа између ADS–B система и људског фактора, као и улога људског фактора у одбрани од сајбер напада (поглавље 6.3). Осим тога, у овом делу, бавимо се и неким изазовима у примени ADS–B, као и будућим правцима развоја ADS–B у контексту оквира за напредно модернизовани ваздухопловни систем.

6.1. ADS–B: ФУНДАМЕНТАЛНИ КОНЦЕПТ

Automatic Dependent Surveillance-Broadcast (ADS–B) је зависан и кооперативан систем за надзор у коме ADS–B транспондер инсталиран у авиону користи SatNav технологију (GPS/GNSS) за периодичну размену (пренос и пријем) важних информације с ATC центрима, као и другим авионима у непосредној околини. Дакле, ADS–B јесте акроним, који означава суштину функционисања протокола [148]. То значи да је ADS–B систем: ***Automatic*** (периодични пренос информација без икакве контроле, тј. учешћа пилота/оператера) и ***Dependent*** (преноси информације, које се односе на позицију и вектор брзине, добијене од GPS/FMS и навигационе авионике), и обезбеђује: ***Surveillance*** (обезбеђује метод за одређивање тродимензионалне позиције и идентификацију авиона, возила или других превозних средстава) и ***Broadcast*** (преноси информације као што су идентитет, положај, брзина, итд., које су доступне свима, а који имају одговарајућу опрему за пријем).

ADS–B протоколом се различити подаци (позиција авиона, брзина, правац, идентификациони број авиона, полазиште и одредиште, итд.), шаљу оближњим авионима и станицама на Земљи преко нешифроване везе за пренос података. У поређењу с традиционалним радарским системима (PSR и SSR) који ажурирају податке о положају сваких 4–5 s, ADS–B емитује информације сваке секунде [413], тако да ADS-B има много већу брзину надзора и тачност у односу на PSR и SSR[165].

6.1.1. ADS–B технологија

Automatic Dependent Surveillance–Broadcast (ADS–B) представља савремени технолошки систем, који обједињује постојећа техничка решења из домена телекомуникација, навигације и осматрања ваздушног простора [10]. Као што је поменуто, овај систем је интегрални део *NextGen* (FAA) и CASCADE (Eurocontrol) програма за унапређење ваздушног саобраћаја, и то у погледу безбедности, економичности, аутоматизације, екологије, итд.

Саставни део ADS–B-а (као и TCAS-а) јесте GPS, тако да ослањање ових *Detect and Avoid* система на GPS, утиче на то да GPS (глава 5) буде један од критичних система у ваздухопловству [305]. Основна GPS услуга, сервисира кориснике с тачношћу локације од око 8 m (95% времена) било где на површини Земљи/близу ње, тако да сваки GPS сателит емитује сигнале пријемницима; локација корисника одређује се из времена које протекне од слања сигнала до његовог пријема. Информације о времену, тј. кодове, преносе сателити, тако да пријемници могу константно одређивати време емитовања сигнала. Сигнал садржи и податке које пријемник може користити за израчунавање локација сателита, као и за прилагођавање, у сврху одржавања тачности. С најмање четири одвојена сателитска преноса, GPS пријемник може триангулисати сопствену 3D позицију, одређивањем растојања (домета) од сваког сателита [415].

[165] На пример, на удаљености од 60 наутичких миља од земаљске станице, прецизност ADS–B је ±20 m, док је прецизност SSR-а ±300 m [414].

Системи за надзор, развијали су се упоредо с развојем ваздухопловстава, и то сви сегменти система за осматрање (сензори, системи за пријем, обраду и дистрибуцију радарске слике и сл.) – од визуелног осматрања и надзора заснованог на радио вези, којом су пилоти јављали своју позицију и тако били надзирани са земље, до прве велике промене условљене појавом RADAR-а (*Radio Detection and Ranging*), за време другог Светског рата, технологије која се заснива на емитовању RF таласа и пријему рефлектованих сигнала, а на основу којих се одређује позиција ваздухоплова. Овај тип радара представља *Primary Survaillance Radar* (PSR).

Primary Survaillance Radar (PSR) је независан, некооперативан надзор и представља најстарију технику аутоматизованог надзора [149, 178, 416]. Примарни радар шаље високофреквентне таласе који се рефлектују од циљева (ваздухоплова) и повратни сигнал прима као ехо [417]; PSR је пасивни систем, што значи да авион не мора имати додатну опрему за функционисање PSR-а. Основни делови PSR-а су предајник, антена, пријемник и процесор сигнала (сл. 27а) [415]. Емитовањем сигнала и обрадом примљеног сигнала, PSR може одредити азимут и курс (коса удаљеност ваздухоплова, тј. растојање између ваздухоплова и радара); азимут се одређује из положаја ротирајуће антене у тренутку примања рефлектованих пулсева, док се курс одређује мерењем временског интервала, од трансмисије пулса до пријема рефлектованих импулса. Међутим, PSR, осим приказа позиције ваздухоплова, даје приказ и других, нежењених објеката, тзв. неред (*clutter*), као што су зграде, јата птица, атмосферске аномалије, итд. ″Неред″ се уклања посебним техникама обраде, применом различитих савремених алгоритама праћења и ″брисања″ сметњи, а на екранима АТС приказују се само покретни објекти, без приказа нежељених фиксних објекта; међутим проблем *clutter*–а још увек није у потпуности превазиђен. Радари се, у зависности од намене, могу поделити на осматрачке **радаре великог домета** и **терминалне** радаре. Први се користе за праћење ваздухоплова на великим удаљеностима; имају 5–15 обртаја антене у минути. Терминални радари су најчешће малог домета и користе се за праћење ваздухоплова у зонама аеродрома. Код ових радара, у односу на осматрачке радаре великог домета, брзина ажурирања података је знатно већа. Основна предност PSR јесте остваривање ваздушног надзора (домет ваздухоплова и азимут), без потребе уграђивања транспондера у авион (део 3.1.2.2). Један од недостатака PSR је непостојање идентификације циља (због недостатка комуникације између PSR-а и опреме авиона), што захтева друге системе/процедуре за корелирање рефлектованих сигнала и детектованих летова. Поред тога, PSR има малу брзину ″освежавања″ података због коришћење механички ротирајуће антене, захтева велику снагу преноса сигнала (јер се исти преносе двосмерно), као и велика финансијска улагања.

Ови проблеми решени су увођењем *Secundary Surveillance Radar* (**SSR**). *Secundary Surveillance Radar*, развијен је најпре за војне потребе (под називом *Identifying Friend or Foo*, IFF), а касније у цивилне сврхе под називом секундарни радар. За разлику од PSR-а, SSR систем састоји се од два главна елемента, и то су: радарски сензор (испитивач/пријемник на земљи) и транспондер (у ваздухоплову) (сл. 27б) [268, 272, 418, 419]. Део опреме на Земљи инсталиран је самостално или у комбинацији са PSR-ом. SSR је кооперативни систем надзора у коме SSR шаље

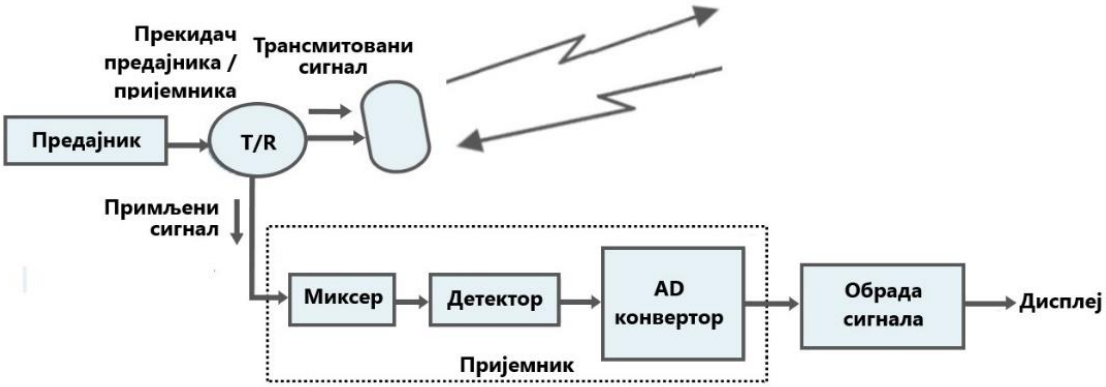
транспондеру ваздухоплова упит на фреквенцији 1090 MHz, док је одговор транспондера на фреквенцији 1030 MHz. Ова комуникациона веза између Земље и транспондера, поред одређивања курса и домета ваздухоплова, омогућава идентификацију ваздухоплова, одређивање његове висине, као и преношење других релевантних информација у зависности од изабраног режима. Постоје три основна **режима рада SSR**-а, означени са **Мод А** (*squawk*), тј. четвороцифрени одговор у режиму А, који представља идентификацију ваздухоплова, затим, **Мод С** (притисак–-висина, тј. добијање података од транспондера о притиску и висини ваздухоплова), као и **Мод S** (селективни), који имају најсавременији SSR, а који, у односу на модове А и С, пружа додатне информације, као што је податак о јединственом идентификатору авиона. Врста информација које се добијају као одговор на испитивање, одређене су режимом рада транспондера. У односу на PSR, коришћење SSR има одређене предности, као што су мања снага преноса (због комуникације између земаљске станице SSR-а и *on-board* транспондера), шири опсег покривености (најчешће 250 NM од радарске локације)[166] и већу брзину ажурирања података. Иако одржавање PSR, захтева мања финансијска улагања од SSR, та цена је и даље висока.

Следећи корак у развоју система за надзор је *multilateration* (**MLAT**) (фуснота 123), кооперативна независна технологија надзора, базирана на *time difference of arrival* (TDoA) принципу – положај авиона се математички израчунава решавањем TDoA једначина, а на основу примљених сигнала (неколико сензора на Земљи) емитованих с транспондера авиона [268, 272]. За коришћење MLAT, нису потребни додатни авио-подсистеми, а за разлику од PSR и SSR, MLAT не користи механички ротирајућу антену, тако да омогућава веома брзо ажурирање података, и даје неопходне информације АТС-у, као што су положај авиона, надморска висина, итд. MLAT систем са широм покривеношћу је *Wide Area Multilateration* (WAM), који се користи у надзору ваздушног простора на рути. У односу на PRS и SSR, MLAT има већу тачност одређивања положаја, у зависности од броја пријемника и њиховог геометријског распореда. Поред тога, трошкови интеграције MLAT и редовно одржавање, много су мањи у односу на застареле радарске системе.

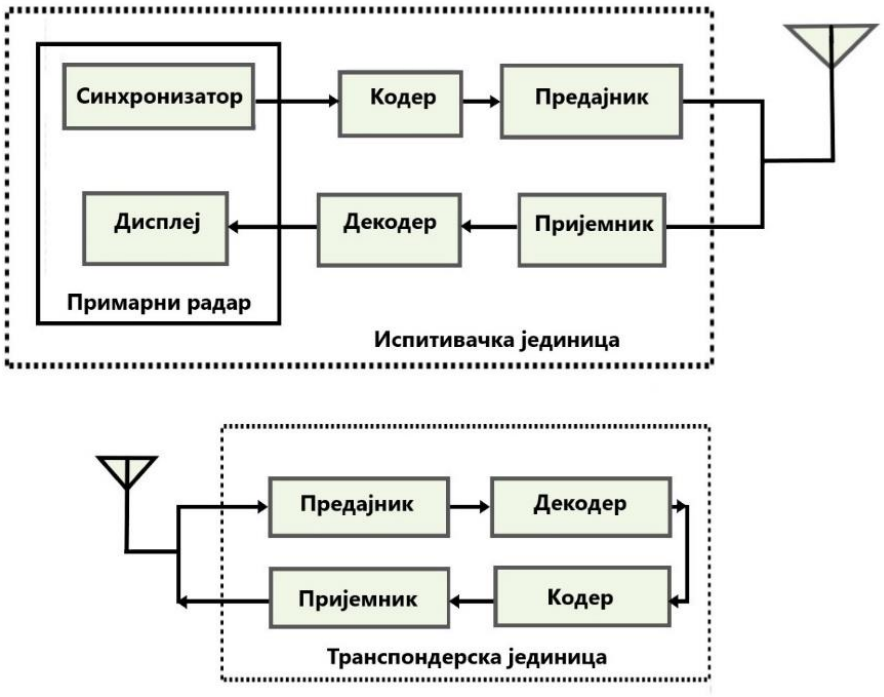
Затим, у напредне технологије спада и *Traffic Collision Avoidance System*, **TCAS**, (део 3.1.2), који функционише независно од АТС и навигационих инструмената [168, 169]. Овај систем односи се директно на појединачни ваздухоплов и омогућава размену информација посебних транспондера, који се налазе у непосредној околини с циљем спречавања колизије. Дакле, овај систем не захтева инфраструкуру на Земљи, али је неопходно да један од два ваздухоплова, који размењују информације, буде опремљен **транспондером** типа **Мод С**.

[166] NM (или M) је ознака за наутичку миљу. То је јединица за дужину (ван SI система), која се, између осталог, користи у ваздухопловству. Према Међународно прихваћеној дефиницији 1 NM = 1852 m.

(а)



(б)

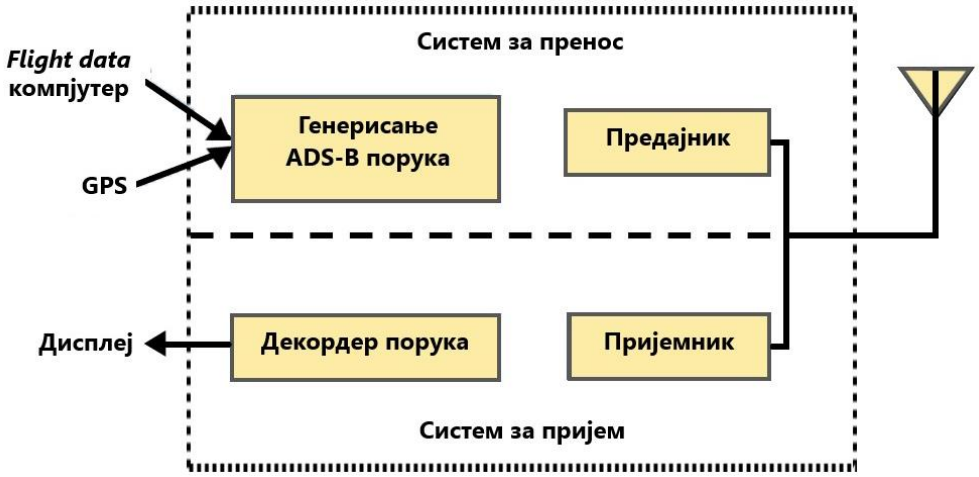


Слика 27. Шематски приказ: (а) *Primary Survaillance Radar* (PSR) и (б) *Secundary Surveillance Radar* (SSR) (модификовано и преузето из [415])

Један од најзначајнијих корака у ваздухопловству, тј. у модернизацији ATC је прелазак на ADS–B [272] бежични комуникациони протокол, развијен као резултат тежње за економичнијим и поузданијим управљањем ваздушним саобраћајем, и за супституцијом радарских система напредним технолошким решењима. ADS–B

јесте савремена технологија, која комбинује постојећа техничка решења из сегмената телекомуникација, навигације и осматрања ваздушног простора[167].

С обзиром на то да је саставни део ADS–B система GNSS (глава 5), ADS–B систем зависи од прецизности овог система. ADS–B је зависни систем надзора, који се користи за периодично одређивање положаја авиона преко навигационих сензора у ваздуху (интегрисани GNSS систем и инерцијална навигација). ADS–B информације емитују се преко проширених сквитера (*squitter*) транспондера Мода С у авиону. Информације о авиону, као што су идентификација, положај, брзина, итд., примају земаљски пријемници АТС-а на 1090 MHz. Врзина ажурирања података за положај и брзину је 2 ажурирања s^{-1}, а за идентификацију, 5 ажурирања s^{-1}. Тако, поред веће брзине ажурирања, ADS–B, у односу на традиционалне радарске системе (PSR и SSR), има много већу тачност одређивања положаја, уз мање трошкове, јер се елиминишу финансијска улагања интеграције и текућег одржавања традиционалних радарских система. Дакле, ADS–B систем повећава безбедност ваздушног саобраћаја – авиони су видљиви у реалном времену за АТС, као и друге ваздухоплове, који имају одговарајућу опрему; омогућава повећање свесности ситуације, као и даје унапређене извештаје о метеоролошким условима, саобраћајном капацитету, приказу саобраћајних информација у пилотској кабини (*Cockpit Display of Traffic Information*, CDTI), избегавању судара у ваздуху, и сл. Блок дијаграм ADS–B дат је на слици 28.



Слика 28. Блок шема ADS–B система (модификовано и преузето из [415])

[167] ADS–B је примарно био намењен за осматрање подручја без радарске покривености. Већина великих аеродрома се налази/окружена је C или B класом вазадушног простора, тј. неопходно је да имају покривеност ≥ неколико стотина фита (1ft=0,3048m). Значајне технологије за осматрање на малим висинама (површинско осматрање) су: *Airport Surface Detection Equipment* (ASDE), који је базиран на принципу PSR (брзина ажурирања података је једно ажурирање s^{-1} и *Airport Surface Detection Equipment, Model* X (ASDE-X), који је базиран на комбинацији PSR, SSR, ADS–B система и MLAT. Ове технологије не обезбеђују квалитетно покривање зона без радарског надзора [178].

У табели 7, сумарно су дате карактеристике различитих техника надзора које се користе у ваздухопловству.

Табела 7. Упоредне карактеристике различитих ваздухопловних система за надзор система (PSR, SSR, MLAT и ADS–B) [149]

Техника надзора	PSR	SSR	MLAT	ADS–B
Концепт рада	Користи рефлектовано ЕМ зрачење (ехо) од ротационе антене	Испитивање/одговор између сензора (SSR ма Земљи и *on-board*)	Математичко израчунавање позиције авиона (TDoA) коришћењем више земаљских сензора	Авион одређује своју позицију, брзину, итд., које шаље сензорима на Земљи
информације	Домет и азимут	Домет, азимут, ID, барометарска висина	3D позиција, идентификација, брзина, итд.	3D позиција, идентификација, брзина, итд
сигнал Фреквенцијска трака	Аналогни 1–2, 2–4 GHz	Дигитални *Uplink* 1030 MHz *Downlink* 1090 MHz	Дигитални *Uplink* 1030 MHz *Downlink* 1090 MHz	Дигиотални 978 MHz 1090 MHz
класификација	Некооперативан, независан	Кооперативан, независан	Кооперативан, независан	Кооперативан, зависан
Брзина ажурирања података	Мала	Мала	Велика	Велика
Стандард протокола	[420]	[272, 420]	[272, 420]	[272, 420]

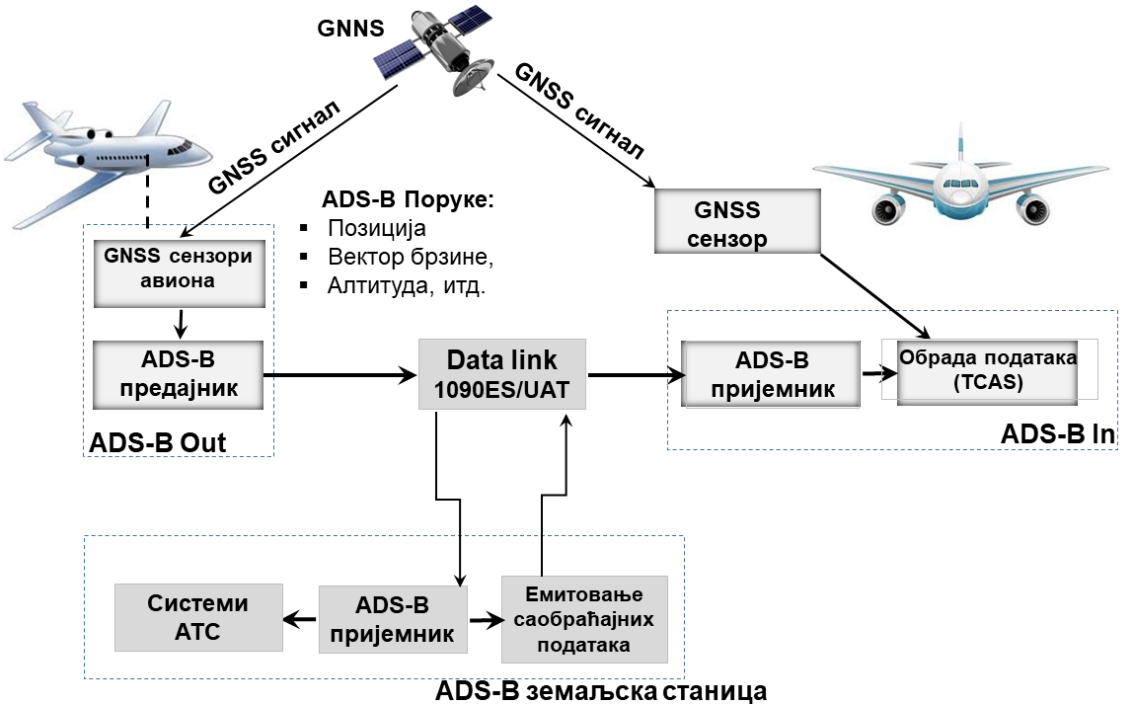
ADS–B протокол обезбеђује међусобну размену емитованих порука између ваздухоплова и АТС земаљских станица. Функционише као предајник (**ADS–B Out**), или пријемник (**ADS–B In**) (сл. 29), тј. има две функције:

- ADS–B Out (емитује информације о авиону, као што су идентификација авиона и позиција у реалном времену, висина и брзина)
- ADS–B In (прима информације о саобраћају и метеоролошким условима од других авиона).

Сваки авион може имати и "In" и "Out" могућности у зависности од врсте транспондера који је инсталиран у ваздухоплов. Ипак, ADS–B In остаје опциона функција, а истовремена примена ADS–B In с другим системима требало би да омогући следеће [422]:

- ADS–B In би требало да побољша безбедност, ефикасност и капацитет ваздушног саобраћаја.
- Две системске интеграције, ADS–B In и *Trajectory-Based Operations* (TBO) требало би да омогуће боље управљање и контролу неких операција у условима велике густине саобраћаја

ADS–B In и *Cockpit Display of Traffic Information* (CDTI), CDTI *Assisted Visual Separation* (CAVS) и *Interval Management* (IM) тренутно обезбеђују повећање ефикасности и представљају велики бенефит за оператере.



Слика 29. Архитектура система ADS–B: ADS-B Out, ADS–B In, *Data link* и земаљских станица (модификовано и преузето из [10, 421])

ADS–B In систем је веома интуитиван, једноставан за коришћење и захтева минималну обуку пилота. Наиме, како су пилоти упознати са системима *Aviation Communication Surveillance Systems* (ACSS) и *Traffic Collision Avoidance System* (TCAS) (описани у делу 3.1.2.2), познати као ACAS (*Airborne Collision Avoidance System*) дисплеји, тако да је прелазак на нове ADS–B In дисплеје, веома једноставан. Међутим, као позадина свега овога остају ADS–B безбедносне рањивости (поглавље 6.2). Стога је од круцијалног значаја повећати безбедност ADS–B система.

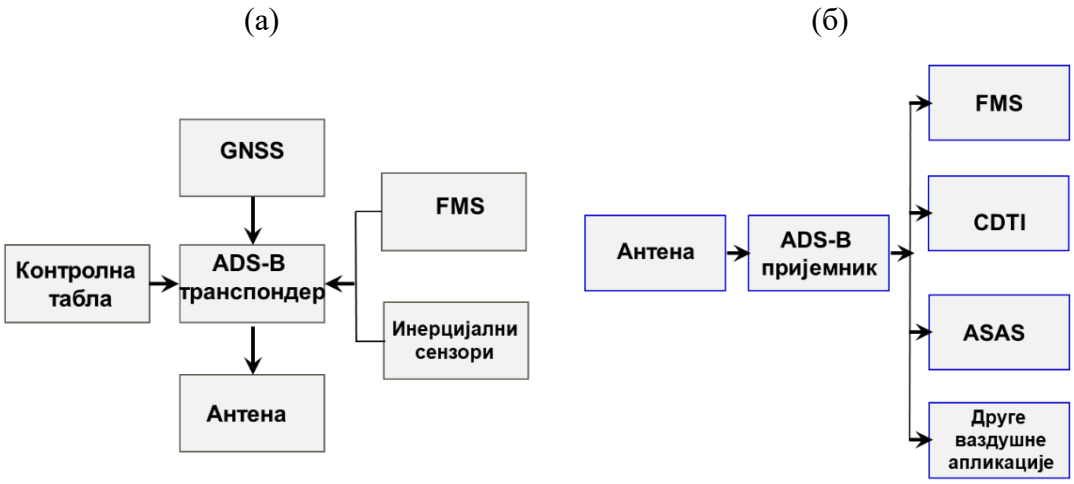
6.1.2. ADS–B инфраструктура и комуникациони протоколи

ADS–B систем се састоји од три међузависна подсистема/компоненте [9–11, 421] (сл. 30):

- Земаљска инфраструктура – *ground based transievers* (GBT) станице (користе се за примо-предају ADS–B информација, које се након пријема колерирају с подацима добијеним из других извора) и антенског систем (омнидирекционална антена, која обезбеђује оперативни домет до 250 NM, што зависи од различитих параметара, као што су конфигурација терена, висина лета, количина података,

распоред пријемника и предајника, опрема ваздухоплова и оперативних процедура.

- Опрема ваздухоплова – ADS–B специјализовани транспондер, GPS,[168] пријемник, висиномер, CDTI, итд. (сл. 30).
- Оперативне процедуре – регулаторна основа за имплементацију и употребу ADS–B система.



Слика 30. Авионика система ADS-B Out (а) и ADS-B In (б) (модификовано и преузето из [10])

Према смеру преношења информација (од/ка ваздухоплову), ADS–B може да функционише као **ADS–B Out** и **ADS–B In**. Прва функција обезбеђује периодично емитовање тачних података о позицији авиона и векторских података заједно са другим информацијама, тј. омогућава аутоматизовани пренос података о параметарима авиона између авиона и АТС, док друга функција омогућава аутоматизовани пренос ових података између авиона, тј. даје приказ ADS–B путања у реалном времену, на дисплеју, у кокпиту авиона. Дакле, ADS–B Out функционише независно и пружа услуге надзора ваздух–земља, тако што периодично шаље позицију и друге информације контролорима АТС или суседним авионима; за разлику од транспондера, ове емитоване ADS–B поруке шаљу се периодично без потребе за упитом, а истовремено их примају и земаљски пријемници, као и пријемници у ваздуху. Подаци добијени из ADS–B порука користе други авиони, који ове податке комбинују са сопственим параметрима, у сврху креирања тродимензионалног вектора стања за израчунавање релативног домета и смера. Кључни предуслови за потпуну примену ADS–B In су сертификација екрана у кокпиту, као и разматрање људског фактора, тј. интеракција човека с аутоматизованим *on-board* системима.

[168] ADS–B опрема, тј. GPS уређај мора бити задовољавајућег квалитета, у циљу добијања што тачније позиције ваздухоплова. У случају да је GPS податак недоступан (из било ког разлога), користи се DME технологија.

Функционисање ADS–B, за разлику од класичног радарског система, веома је једноставно и заснива се на следећем: ваздухоплов опремљен ADS–B системом помоћу GNSS сензора (у ваздухоплову) прима податак о сопственој позицији, који се шаље ADS–B транспондеру, а који овај податак, као и друге информације (параметри лета, идентификација, итд.) прослеђује (периодично, најчешће два пута у секунди), у формату поруке 1090EC/UAT, корисницима (другим авионима и земаљским станицама опремљеним ADS–B-ом). Транспондер добија и друге податке (на пример метеоролошке) са Земље, као и од ваздухоплова. Сви коришћени телекомуникациони линкови веома су поуздани и широко-појасни, тако да су елиминисани проблеми у вези с дометом, сметњама и временским интервалом ажурирања информација. За потпуну обраду и размену ADS–B порука, земаљске ATC станице и суседни авиони морају бити опремљени са системом ADS–B In. Сваки авион може имати и ″In″ и ″Out″ могућности, у зависности од тога која је опција инсталирана у авиону.

Функција **ADS–B In,** као што је поменуто, је **опциона услуга**, којом се омогућава да ваздухоплов добија податке, који се приказују на CDTI интерфејсима, најчешће MFD (део 3.1.2.2) и EFB (фуснота 78) уређајима, а које емитује други ваздухоплов из непосредне околине. Ове информације користи и TCAS систем [423]. Функција ADS–B Out омогућава емитовање статусних информација о ваздухоплову. Наиме, ADS–B транспондер прикупља податке о екстерном и интерном стању ваздухоплова (локација, алтитуда, курс, итд.), које процесор обједињује и шаље циљевима, тј. ваздухопловима у околини и станицама на Земљи; ADS–B транспондери прослеђују податке о стању ваздухоплова независно и периодично (у тачно дефинисаним временским интервалима) за разлику од SSR код кога транспондер одговара само по захтеву/упиту секундарног радара.

ADS–B систем (ADS–B In/Out) према утврђеним стандардним протоколима, преноси поруке које садрже велики број података, тј. информација (подаци добијени од ваздухоплова и земаљских станица, поруке TIS–B (*Traffic Information System – Broadcast*) система, као и остале поруке FIS–B (*Flight Information System – Broadcast*) система, који садрже метеоролошке податке, NOTAM-е и сл.)., као што су позивни знак, јединствена 24-битна ICAO адреса, гео-позиција, висина, итд. [178]. На основу ових информација, станице на Земљи врше мониторинг ваздушног саобраћаја.

Поред зависности од **навигационог система** (GPS је најшире коришћени навигациони систем у ADS–B), ADS–B у великој мери зависи од комуникационих система. Користе се три врсте *data* линкова: 1090 MHz *extended squitter* (1090-ES), 987 MHz *Universal Access Transceiver* (UAT) и VHF *Datalink Mode 4* (VDL-M4); коришћена врста протокола, зависи од врсте ваздухолова, а у складу са смерницама FAA [411]. Најраспрострањенија комуникациона веза за пренос података је 1090-ES.

Домет ADS–B земаљских радио станица зависи од тога на којој је висини авион и свих препрека које се налазе између њих (номинални домет без икаквих препрека је око 150 NM). Тако, ″покривеност″ ADS–B, ограничена је тренутном удаљеношћу авиона од доступних земаљских ADS–B станица, као и других авиона. Како не

постоји посебна енкрипција ADS–B података, исте може примити сваки пријемник на адекватној фреквенцији. Најпоузданије информације о околном саобраћају обезбеђује се директном комуникацијом ваздух–-ваздух преко ADS–B, која је могућа само уколико оба авиона емитују на истом линку (978 MHz/1090 MHz). Уколико авион, унутар одређеног домета другог авиона, не комуницира на истој вези, било која земаљска станица (у домету) и даље може да обезбеди овим авионима *Automatic Dependent Surveillance – Rebroadcast* (**ADS–R**) податке, све док је авион унутар ефективног домета ADS–B преноса. Слична технологија ADS–R-у, је *Traffic Information System – Broadcast* (TIS–B), али за разлику од ADS–R система, **TIS–B**, емитује податке о авионима који нису опремљени са ADS–B (опремљени су само транспондерима). Тако, авиони који имају ADS–B Out/In, надзорне информације о другим авионима који нису опремљени са ADS–B, обезбеђује услуга TIS–B[169]. Дакле, због постојања различитих формата порука и различитих *data link* модова, ADS–B земаљске станице треба да обезбеде услуге ADS–R и TIS–B [424, 425].

Комуникација у оквиру ADS–B, као што је поменуто, остварује се коришћењем утврђених (стандардизованих) комуникационих протокола, а најважнији су 1090-ES[170], 987 MHz UAT[171] или VDL-M4[172]. Према захтевима FAA, коришћена врста протокола, зависи од типа ваздухоплова (нпр., 1090-ES протокол се користи за приватне и комерцијалне оператере, односно ваздухоплове високих перформанси, док се UAT користи за генералну авијацију), док се у Европи, државе самостално опредељују за један од постојећих протокола, али је у CASCADE програму, основни протокол 1090-ES [178].

ADS–B 1090-ES протокол[173] (сл. 31) развијен је на тренутном режиму протокола S транспондера (компатибилан је са стандардима SSR и TCAS система). UAT протокол се разликује од 1090-ES протокола и мање је заступљен у ADS–B, јер захтева интеграцију потпуно нове опреме.

---

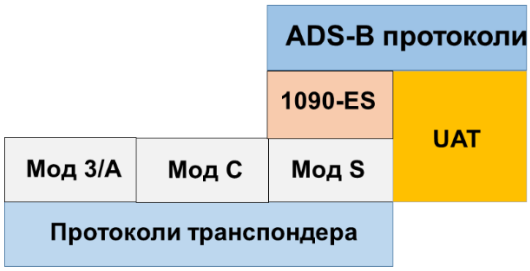
[169] За коришћење FAA услуга TIS–B и ADS–R, потребно је да авион будите у региону у коме се нуди услуга TIS–B, затим, да емитује валидне податке о позицији (у последњих 30 s) FAA SBS (*Surveillance and Broadcast Services*), као и буде опремљен с ADS–B.

[170] 1090-ES протокол, углавном се користи за комуникацију изнад 18.000 FT (FL180). Како је исти комуникациони канал већ заузет овим сервисима, постоји проблем капацитета комуникационог линка (ES порука садржи 112 бита, док стандардна порука 1090 одговора садржи 56 бита, што значи да у 1 s може послати максимално 5 пуних порука). Протокол 1090-ES не подржава FIS–B (јер није бидирекционални).

[171] UAT протокол омогућава бидеркционалну комуникацију; подржава проток информација ≤ 100 kbs^{-1}, тако да подржава све ADS–B сервисе. Данас се користи за комуникацију испод 18.000 FT (FL180).

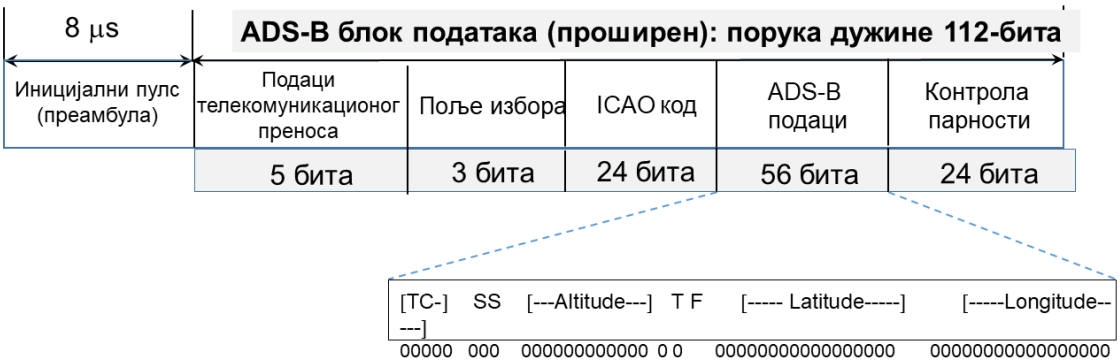
[172] VDL-M4 протокол, најчешће коришћен на територији Европе, употребљава се у фреквенцијском опсегу 108–117,975 MHz и комуникационим каналима од 25 KHz. Сматра се да ће овај протокол, због недостатака (мали пропусни опсег, неопходност потпуно нове опреме, веома мали домет) бити потпуно превазиђен.

[173] 1090-ES протокол је најшире у употреби јер његова имплементација у ваздухоплове не захтева уградњу новог хардвера, већ само софтверске модификације постојећег.



Слика 31. Однос протокола режима транспондера и ADS–B протокола (модификовано и преузето из [426])

ADS–B Out шаље поруке сваке секунде брзином 1 Mbit/s преко 1090-ES или UAT [409]. ADS–B има протокол отвореног приступа (добра интероперабилност), али његове поруке имају незадовољавајући ниво шифровања: последња 24 бита укључују проверу паритета која детектује и исправља грешке у преносу порука (сл. 32) [18, 411, 427, 428].



Слика 32. ADS-B порука: структура проширене поруке дужине 112 бита (модификовано и преузето из [18])

Свака ADS–B порука садржи преамбулу (иницијални импулс, тј. сигнал, који се у комуникацијама заснованим на мрежама, користи за синхронизацију времена преноса између два или више система) од 8 μs за синхронизацију и 56-битни (кратки) или 112-битни (проширени) блок података. Дакле, проширена ADS–B порука има 112 битова, које се преносе путем 1090 MHz (″проширен сквотер″) *data* линкова [411].

Формат (оквир)[174] ADS–B протокола с поруком, која се састоји од 112 битова, приказан је на сл. 32 [18]. ADS–B оквири садрже:

- преамбулу (у трајању од 8.0 μs) – користи се за синхронизацију предајника и пријемника

[174] Оквир – јединица за дигитални пренос података у телекомуникацији и рачунарским мрежама.

- 112-битни *payload*[175], састоји се од пет сегмената/поља, и то:
  - први, 5-битни сегмент, који садржи податке телекомуникационог преноса и односи се на формат *downlinka* (DF), а који се користи за кодирање емитованих порука (ADS–B проширени сквотер користи DF = 17)
  - други, 3-битни сегмент је поље избира
  - трећи, 24-битни сегмент садржи јединствену адресу ваздухоплова

    Следећих 56 битова (ADS–B подаци) односи се на податке подсегмената, и то: идентификацију лета (позивни знак, FI), положај (географска ширина/дужина, POS), тачност позиције (GPS хоризонтални заштитни лимит, PI), барометарску и геометријску висину (BGA), вертикалну брзину (VR), угао путање и *graund spead* (TAGS), *emergency* индикацију у случају селектовања *emergence* kôda (EI) и специјална идентификација позиције када је селектован IDENT (SPI) [427]. ADS–B поруке нису енкриптоване: последњих 24 битова укључује проверу парности, која детектује и коригује емитоване грешке у порукама. Дакле, ADS–B има протокол отвореног приступа (добра интероперабилност), али његове поруке имају незадовољавајући ниво шифровања, јер последња 24 бита укључују проверу паритета која открива и исправља грешке у преносу порука [18, 411, 427, 428] Овом 24-битном информацијом и помоћу фиксног генераторског полинома степена 24, пријемник ADS–B порука може исправити могуће грешке (до 5 битова грешака) у 1090-EC протоколу [413]. Међутим, свака порука с више од 5-битова грешака сматра се оштећеном и таква порука се одбацује. На основу података о брзини одбацивања порука у ADS–B мрежи из 2017. год. [13], закључује се да велики број битова у грешкама у ADS–B порукама су резултат преоптерећења ADS–B комуникационих веза за пренос података.

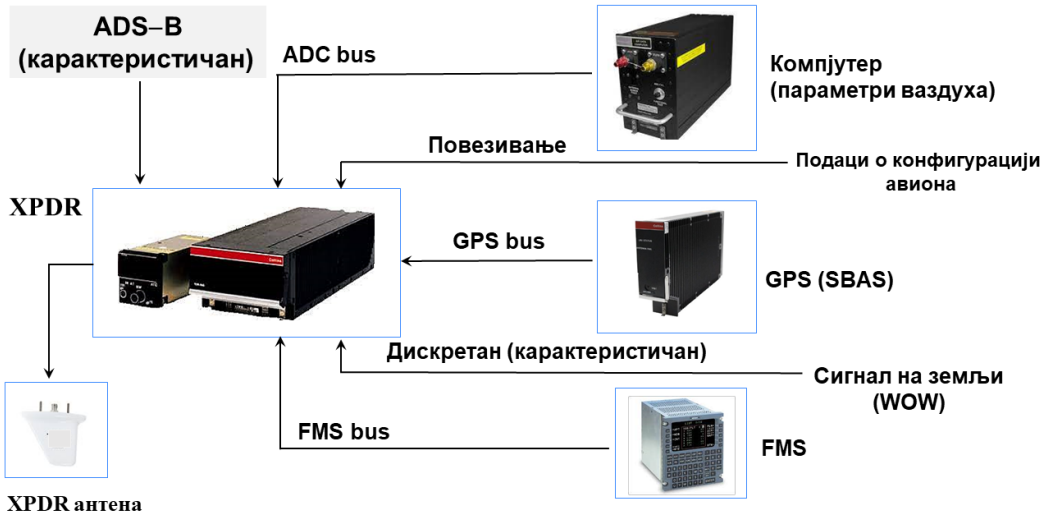
6.1.3. ADS–B подаци

ADS–B подаци преносе се ″аутоматски″ (без испитивања од стране земаљских станица), SSR транспондером (који је повезан с различитим изворима података (сл. 33).

Извор података (подаци у вези с параметрима ваздуха, као што су притисак, индицирана ваздушна брзина, права брзина, вертикална брзина и баро-корекција), је компјутер за податке из ваздуха (*Air Data Computer*, ADC). Транспондер (XPDR) је кодиран и конфигурисан за: 24 *bit* ICAO адресу, категорију емитера (нпр. лаки авион), дужину и ширину авиона, лонгитудинални *offset* GPS антене, карактеристике *on board* линка за пренос података, карактеристике уграђеног ACARS-а и ниво *System Design Assurance* (SDA). GPS/SBAS, даје транспондеру, осим Позиција, Брзина и Време (PVT) и друге квалитативне податке, као што су:

[175] *Payload* – у рачунарству и телекомуникација, односи се на део пренетих података, који представљају стварну (послату) поруку, док заглавља и метаподаци омогућавају испоруку *payload*-а.

латитуда, лонгитуда, брзина, UTC време[176], Угао путање/кретања, Висина геоида, Лимити интегритета – аналитички подаци. За добијање информација у вези са детекцијом ваздух–-земља, тј. да ли је авион на Земљи или у ваздуху, користи се *Weight On Wheels* (WOW) прекидач, на стајном трапу. FMS (*Flight Management System*) обезбеђује следеће податке за транспондер: селектовани наслов, изабрану надморску висину, нагиб, промена угла кретања, прави курс и висину по радио-висиномеру. Опционо, може се инсталирати прекидач за укључивање/искључивање ADS–B, у циљу могућности за прекид преноса ADS–B података (не приказивање на дисплеју за надзор), уколико се нпр. детектује да су исти нетачни/лажни.



Слика 33. Блок дијаграм уграђене ADS–B опреме у авион (комуникацијски протокол 1090ES) (слика модификована и преузета из [429])
XPDR – транспондер; FMS – *Flight Management System*; WOW – *Weight On Wheels*; SBAS – *Space Based Augmentation System*; ADC – *Air Data Computer*

Подаци који се достављају транспондеру, интерно се чувају у *Binary Data Store* (BDS)[177], као што су *BDS 05h Airborne Position, BDS 06h Surface Position, BDS 08h A/C Id & Category, BDS 09h Airborne Velocity, BDS 62h Target State and Status Message*, и *BDS 65h Aircraft Operational Status*. Ове поруке преносе се различитим брзинама преноса, у зависности од статуса: ваздух, AIR (сваких у 0,5 s) и земља, GND (сваких 0,5 s или 5 s, уколико се авион креће, или се не креће, редом). Одређивање AIR/GND статуса је засновано на WOW прекидачу, као и

[176] UTC (*Universal Time Coordinated*), је најпрецизнији и најчешће коришћени стандард за време, који се користи глобално од 70.-их година 20. века, а који је заменио раније коришћено средње време по Гриничу (*Greenwich Mean Time*, GMT) UTC формат садржи 2 цифре за час на основу 24-часовног сата, након чега следе две цифре за минуте и две цифре за секунде, раздвојене двотачкама.
[177] Дефинисано је 256 интерних BDS регистара (сваки садржи 56 бита ADS–B података). Транспондер брише интерне регистре, уколико се одговарајући садржај података не ажурира у одређеном временском периоду.

информацијама о брзини и радио-висиномеру[178]. Поред тога, статус AIR/GND одређује и информације које порука садржи. За коректан пренос ADS–B података, неопходна је адекватно одређивање статуса AIR/GND.

Информације о позицији преносе се коришћењем алгоритма за компримовање података. У оквиру поруке о позиција у ваздуху/на површини, ширина и дужина се преносе са 17 бита. За добијање прецизнијих података о позицији, неопходно је 34 бита, због чега се примењује алгоритам за *Compact Position Report* (CPR), а сложеност алгоритма може довести до погрешне индикације позиције.

Сви улазни подаци транспондера могу се извести у ASCII текстуалну датотеку[179]. GPS UTC се користи за временску синхронизацију снимака, док се скуп параметара, излазна брзина и јединица, могу појединачно конфигурисати према потреби, као што је нпр. дато у Табели 8.

ADS–B је сложен систем, тако да постоји велика вероватноћа за пренос погрешних података. С друге стране, ATM систем добија податке из различитих система, као што су SSR, MLAT, PSR и ADS–B. Због тога, подаци о позицији, које дају различити системи, уносе се у алгоритам (нпр. *Kalman* филтер, видети део 6.2.2) који израчунава највероватнију позицију авиона. Омогућавање адекватне фузије сензора (и у случају ADS–B података који нису у корелацији с другим системима за надзор) од суштинског је значаја и требало би да буде предмет ADS–B инспекције лета.

Теоретски, ADS–B је идеалан систем за надзор ваздушног саобраћаја, али у реалности, постоје проблеми у анализи ADS–B података, које трансмитују различити авиони [429]. ADS–B обезбеђује огроман број података/параметара, тачних, али и нетачних, који се користе за надзор. Узрок преношења нетачних података, могу бити различити, као нпр. некомпатибилност између транспондера и повезане GPS/FMS опреме, која мора бити тестирана и одобрена у погледу усаглашености са захтевима ADS–B. Модификација неког од извора података ADS–B или транспондера (нпр. надоградња FMS софтвера или GPS пријемника), захтева поновно тестирање свих функција ADS–B-а; за проверу адекватног фунционисања ADS–B, неопходно је детаљно познавање садржаја ADS–B поруке. Такође, узрок преношења нетачних података може бити нетачан унос података у транспондер (RFI сметње GNSS-а, као што су ометање или лажирање, које узрокују недоступност ADS–B-а), проблем с транспондером (нпр. нетачна екстраполација позиције), затим, проблем у вези с GNSS пријемником, као и систематски проблеми с одређеним типом авиона. За елиминисање нетачних података ADS–B-а, авионе

[178] Најчешће, AIR/GND статус одређује WOW прекидачем, али у случају да је брзина на земљи/назначена ваздушна брзина већа од 100 kts, транспондер аутоматски прелази у AIR режим, што би требало да обезбеди адекватан пренос података у случају блокираног WOW прекидача. За прелазак на режим AIR неки транспондери такође процењују информације на основу радио висине (када су исте веће од 50 ft).

[179] ASCII (аски) је амерички стандардни кôд за размену података, кога сачињава скуп карактера (кодова), а који се најчешће користи у примени рачунара. Утврђен је као међународни стандард, ISO–7 (за кодирање се користи 7 битова, односно 1 бајт); са 7 битова може се представити 2^7 =128 различитих знакова.

тестира особље за одржавање авионике након инсталирања ADS–B-а, а ове тестове, неопходно је поновити након сваке промене извора података за ADS–B.

На основу изведених захтева за ADS–B проверу лета одређеног авиона, транспондер који подржава ADS–B интегрише се у компјутерски систем AFIS (*Automated Fingerprint Identification System*). За разлику од стандардне инсталације, (сл. 33) AFIS рачунарски систем у реалном времену (*Realtime computer System*, RTS) користи се као извор података за транспондер. AFIS опреме за ADS–B проверу лета авиона. RTS прима *Air Data Computer* (ADC), GPS и FMS податке од авионике и директно их прослеђује транспондеру. Улазни сигнал WOW може се одвојено контролисати RTS-ом, независно од правог прекидача WOW на стајном трапу ваздухолова. На овај начин, омогућено је емитовање ADS–B ваздух (AIR) и земља (GND) порука, као и симулација проблема с WOW прекидачем. Повезивање авиона остварује се конектором. Режим (мод) S адреса је конфигурисана за конектор, као и за специфичну ADS–B конфигурацију за дати авион (нпр. *System Design Assurance* (SDA) ниво, категорија емитера, лонгитудинални *offset* (помак) GPS антене, ширина и дужина авиона). Инсталирањем конектора с различитим везама, могу се симулирати друге врсте авиона.

Релевантни параметри перформанси ADS–B могу се ″изменити″ од стране корисника/оператера користећи AFIS софтвер у циљу симулације незадовољавајућег или изузетно доброг квалитета навигације, и то: положај (с конфигурабилним *Position Offset* за креирање помака према SSR/PSR), барометарска висина (*Baro. Pressure Altitude*), GNSS алтитуда, хоризонтална граница заштите (*Horizontal Protection Limit*, HPL) за модификовани NIC[180], хоризонтални аналитички подаци (*Horizontal Figure of Merit*, HFOM) за модификовани NACp[181], аналитичке податке за хоризонталну брзину (HFOM *Velocity*) за модификовани NACv[182] и VFOM. AFIS софтвер омогућава/онемогућава пренос ADS–B података, тако да је могуће симулирати губитак ADS–B излаза, без губитка одговора SSR-а – транспондер и даље одговара на упит SSR-а, али не преноси ADS–B податке

Као што је поменуто, сви улазни подаци транспондера могу се извести у ASCII текстуалну датотеку за евалуацију података након лета, за поређење с ADS–B или ATM снимцима са земље.

[180] NIC (*Navigation Integrity Category*): одржавање интегритета радијуса HPL с вероватноћом од 95%.
[181] NACp (*Navigation Accuracy Category for Position*) је 95%-тни интервал поузданости позиције.
[182] NACv (*Navigation Accuracy Category for Velocity*): 95% интервал поузданости брзине, базирана на аналитичким подацима за хоризонталну брзину.

Табела 8. ASCII параметри (ASCII file: ADS-B transponder+call_sign+date and time.txt; frequency: 1Hz (10Hz) (Добијено љубазношћу SMATSA)

Б	Назив	Значење	Јединица	Опис
1	Time	Time		UTC Time from real time computer
2	GPS Time UTC	GPSTime_UTC		GPS Time from reference position HH:mm:ss:SSS
3	XPDR ADC Baro Alt.	XPDRAdcBaroAltitude	[ft]	Transponder Baro altitude from Air Data Computer
4	XPDR ADC Mach No.	XPDRAdcMachNumber	[]	Transponder Mach number from Air Data Computer
5	XPDR ADC computed Air speed	XPDRAdcComputedAirSpeed	[kts]	Transponder computed air speed from Air Data Computer
6	XPDR ADC true Air speed	XPDRAdcTrueedAirSpeed	[kts]	Transponder true air speed from Air Data Computer
7	XPDR ADC altitude rate	XPDRAdcAltitudeRate	[kts]	Transponder altitude rate from Air Data Computer
8	XPDR ADC static Air Temperature	XPDRAdcStaticAirTemperature	[deg]	Transponder static air temperature from Air Data Computer
9	XPDR ADC Baro corr.	XPDRAdcBarometricCorrection	[hPa]	Transponder barometric correction from Air Data Computer
10	XPDR GPS Latitude	XPDRGpsLatitude	[deg]	Transponder latitude from GPS
11	XPDR GPS Longitude	XPDRGpsLongitude	[deg]	Transponder longitude from GPS
12	XPDR GPS NS velocity	XPDRGpsNsVelocity	[kts]	Transponder N-S velocity from GPS
13	XPDR GPS EW velocity	XPDRGpsEwVelocity	[kts]	Transponder E-W velocity from GPS
14	XPDR GPS GNSS time	XPDRGpsGnssTime	[s]	Transponder GNSS time from GPS
15	XPDR GPS HIL	XPDRGpsHil	[NM]	Transponder Horizontal Integrity Level from GPS
16	XPDR GPS HFOM	XPDRGpsHfom	[NM]	Transponder Horizontal Figure Of Merit from GPS
17	XPDR GPS HFOM Vel.	XPDRGpsHfomVelocity	[kts]	Transponder velocity HFOM from GPS
18	XPDR GPS Track angle	XPDRGpsGnssTrackAngle	[deg]	Transponder GNSS track angle from GPS
19	XPDR GPS Ground Speed	XPDRGpsGnssGroundSpeed	[kts]	Transponder GNSS ground speed from GPS
20	XPDR GPS Altitude	XPDRGpsGnssAltitude	[ft]	Transponder GNSS altitude from GPS (WGS-84)
21	XPDR GPS Vertical velocity	XPDRGpsGnssVerticalVelocity	[ft/min]	Transponder GNSS vertical velocity from GPS
22	XPDR GPS VFOM	XPDRGpsVfom	[ft]	Transponder Vertical Figure Of Merit from GPS
23	XPDR FMS True Heading	XPDRFmsTrueHeading	[deg]	Transponder True heading from FMS
24	XPDR FMS Magnetic Heading	XPDRFmsMagneticHeading	[deg]	Transponder Magnetic heading from FMS

25	XPDR FMS Aircraft Registry Word1	XPDRFmsAircraftRegistryWord1	[HEX]	Transponder Aircraft Registry Word1 from FMS
26	XPDR FMS Aircraft Registry Word2	XPDRFmsAircraftRegistryWord2	[HEX]	Transponder Aircraft Registry Word2 from FMS
27	XPDR FMS Aircraft Registry Word3	XPDRFmsAircraftRegistryWord3	[HEX]	Transponder Aircraft Registry Word3 from FMS
28	XPDR FMS Roll Angle	XPDRFmsRollAngle	[deg]	Transponder Roll angle from FMS
29	XPDR FMS Ground Speed	XPDRFmsGroundSpeed	[kts]	Transponder FMS ground speed from FMS
30	XPDR FMS Track angle rate	XPDRFmsTrackAngleRate	[deg/s]	Transponder FMS track angle rate from FMS
31	XPDR FMS Vertical speed	XPDRFmsVerticalSpeed	[ft/min]	Transponder FMS vertical speed from FMS
32	XPDR FMS Selected Heading	XPDRFmsSelectedHeading	[deg]	Transponder FMS Selected Heading from FMS
33	XPDR NA Cp	XPDRFNACp	[/]	Transponder Navigation Accuracy Category for Position
34	XPDR NA Cp	XPDRFNACv	[/]	Transponder Navigation Accuracy Category for Velocity
35	XPDR NI C	XPDRFNIC	[/]	Transponder Navigation Integrity Category
36	XPDR Status ADSB ON	XPDRStatusADSBOn	[/]	Transponder status of “Send ADS-B”
37	XPDR Status WoW	XPDRStatusWoW	[/]	Transponder status of “Weight on Wheels”

6.1.4. ADS–B имплементација

Од глобалног плана до реалности, имплементација ADS–B Out се активно одвијала у многим регионима света. Према ICAO, употреба ADS–B дозвољена је искључиво када се процени да ADS–B перформансе у одређеном ваздушном простору, превазилазе неопходни ниво [148]. Ово се нарочито односи на безбедносни аспект имплементације ADS–B (поглавље 6.2). С обзиром на то да се перформансе система могу временом погоршати из различитих разлога, периодична процена безбедности ADS–B система је од суштинског значаја, што укључује надгледање ADS–B земаљских станица, авионике и нивоа перформанси. Такође, имплементација ADS–B In захтева потпуно оперативан ADS–B Out, сертификацију екрана кокпита, разматрање људских фактора (пилот) и друге активности за које су неопходни дужи рокови остваривања планираних активности.

Потпуно функционалан ADS–B систем (ADS–B Out и ADS–B In), захтева опремљеност авиона сертификованом ADS–B авиоником, затим, сертификоване земаљске ADS–B станице с потпуном покривеношћу ваздушног простора, као и глобално установљене оперативне процедуре и мандате. Испуњеност ових захтева зависи од авио-оператера (опремљеност ваздухоплова адекватном опремом), пружаоца услуга ваздушне навигације (обезбеђивање земаљске инфраструктуре) и

регулатора (специфицирање оперативних процедура и додељивање мандата различитим заинтересованим странама). При свему овоме, кључна је спремност произвођача опреме да развијају функционалности, које подржавају ADS–B. Поред тога, за потпуну оперативност ADS–B система обавезна је и сарадња између пружаоца услуга ваздушне навигације и авио-оператера, што је од круцијалног значаја за остваривање захтеваних перформанси система и безбедносних аспеката предвиђених апликација.

Ипак, упркос очекиваним предностима ADS–B, усвајање и примена овог система одвијала/одвија се у фазама, а с обзиром на сложеност имплементације, учешће бројних заинтересованих страна, као и неопходне финансијске трошкове. Свакако, неопходан је глобални мандат за пружање комплетне услуге ADS–B система, јер ће у противном, ATC морати да функционише у мешовитом оперативном окружењу (тј. радар и ADS–B) са онемогућеном функцијом ADS–B In.

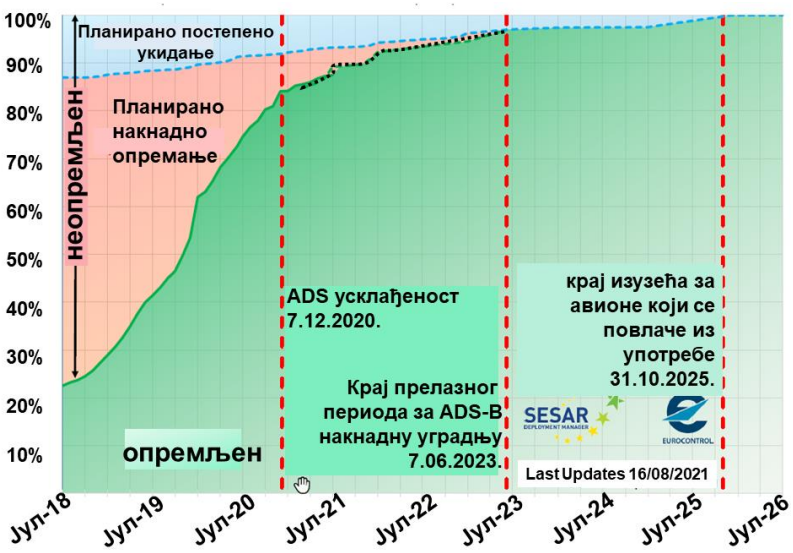
Рок за имплементацију ADS–B Out у USA, била је 2020. година. Систем ADS–B In, остаје опциони из неколико практичних разлога, као што су трошкови имплементације, као и различити стандарди опреме и захтеви за кокпит. С обзиром на погодности које нуди, може се рећи да се с нестрпљењем очекује завршетак имплементације целог ADS–B система, тј ADS–B Out/In система.

Програми модернизације пројеката као што су EUROCONTROL-ов SESAR и FFA-ов NextGen (део 3.1.2.1), имају заједнички основни циљ – повећање капацитета ваздушног простора и безбедност без штетног/опасног окружење [411], тј. имплементацију ADS–B система.

Свакако, 2020. година ће остати упамћена као прекретница у историји ваздухопловства, и то не само с обзиром на мандат ADS–B постављен од стране FAA и EASA, већ и као година у којој је пандемија (Covid-19) изазвана новим корона вирусом SARS-CoV-2 у 2019. години, довела до драстичне промене у авијацији, генерално, драматично смањивши промет путника на глобалном нивоу [430], као и имобилишући бројне авионе, с обзиром на то да су планови управљања флотом били значајно измењени на начин да су поруџбине отказане, а авиони ишли у ″превремену пензију″. Анализа ефеката Covid-19, као што су еколошки и еколошко-економски утицај на комерцијалну авијацију [431] и утицај људског фактора на одржавање неопходне авио-безбедности [432], као и анализа тренутне ситуације у ваздушном саобраћају на глобалном нивоу, а која се односи на ажурирања авио-опреме, ADS–B апликације, управљање флотом од стране авио-компанија, итд., добијених на основу широког скупа података о ваздушном саобраћају од стране потпуних OpenSky *data*, могу се наћи у најскорије објављеним научним радовима [430, 433, 434].

Европска комисија, мандатом, познатим као SPI IR, захтева од авио-оператера да авионе опреми посебним функцијама надзора, у циљу трансформације европске инфраструктуре за надзор, у моћнију ADS–B технологију. SESAR *Deployment Manager*, почевши од децембра 2018. године, континуирано ажурира план на годишњем нивоу. Према SESAR-у, проценат имплементације опреме ADS–B,

тачније ADS–B верзије 3, је била 87,6% (август 2021.) и обухватала је авионе који подлежу мандату SPI IR, као и регистроване у EU27+4 (сл. 34) [435].



Слика 34. Еволуција опреме ADS–B (EU27+4): планирано опремање/уградња (тачкаста линија), планирано постепено укидање (испрекидана линија) и постојећа опрема (пуна линија), према CECAP-у (слика модификована и преузета из [435])

Поред тога, а у вези са **имплементацијом опреме** на Земљи, SESAR је пратио доступну ADS–B покривеност на Земљи, која укључује одвојене земаљске ADS–B станице, као и WAM системе, аеродромске мултилатерационе системе и радаре режима S (сви поменути системи имају ADS–B могућности). За постизање предвиђене покривености, постављање ADS–B сензора у циљу њихове интеграције у систем надзора ADS–B података, још је један од важних корака за ANSPs. Уколико је интеграција оговарајуће синхронизована по доменима и подржана адекватним програмом у циљу генерисања планови за улагања на Земљи, онда се претпоставља да ће већина флоте комерцијалног ваздухопловства EU бити опремљена ADS–B системом, као и да су најважнија регулаторна и техничка питања у различитим доменима (земаљски, ваздушни и свемирски) адекватно решена. До краја 2023. године већина ANSP-ова у Европи, могла би започети са пружањем услуге раздвајања у комерцијалном ваздухопловству заснованом на ADS–B-у, као што је и назначено 2019. године.

Глобално, различити ADS–B мандати су већ успостављени, или се очекују. Мапа глобалног мандата [435], редовно се ажурира и одржава, и приказује регионе с различитим захтевима (најмање ADS–B верзија 0 за Аустралију, Монголију, Индију, Вијетнам, Индонезију, Малезију и Папуа Нова Гвинеја, и ADS–B верзија 2 за USA, EU, Јужну Африку, Мексико, Колумбију и Нови Зеланд). Такође, на сл. 34, дати су и предвиђени датум ступања на снагу, текуће регулаторне активности и мандати који се планирају у блиској будућности (Канада, Кина и Саудијска Арабија).

У времену које долази, све већи број летелица ће егзистирати у ваздушном простору, што ће резултирати његовом огромном заузетошћу, као и порастом броја ADS–B порука. Сходно томе, постоји много изазова у перспективи, као што је онај који се односи на то како избећи преоптерећење канала и губитак порука на фреквенцијском опсегу 1090 MHz, односно омогућити ефикасност или брзо и тачно примање и обраду ADS–B порука. Један од будућих развојних трендова је свемирски ADS–B, релативно новија технологија заснована на коришћењу мреже сателита за обезбеђивање ADS–B покривености ″одозго″ [436]. Дакле, да би се постигао надзор ADS–B система заснованог на сателитској матрици, информације које шаљу авиони прима сателитски ADS–B, који ове извештаје прослеђује земаљској станици преко сателитског комуникационог канала. Први светски пружалац услуге за океанско раздвајање авиона је *Aireon*, сертификован маја 2019. године од стране EASA као нови ANSP према којем је *Aireon* први лиценцирани провајдер. Убрзо након тога, EUROCONTROL и *Aireon* су склопили аранжман који се односи на коришћење свемирских ADS–B података како би се побољшало управљање протоком ваздушног саобраћаја у Европи.

Сада, када је мандат ADS–B Out постао пропис, појавили су се одређени проблеми, као што је проблем *Flight ID issue* (*Call Sign Mismatch*, CSMM). Ово ″неподударање позивних знакова″, за FAA, као и за кориснике ваздушног простора у свим сегментима, биће нарочити проблем, због све већег коришћења нових ADS–B In апликација, као што је *Interval Management* [437]. Према FAA, основни узроци CSMM-а су нетачно програмирано поље ID лета ADS–B примо-предајника током инсталације, употреба необичних позивних знакова и CSMM-а који се јављају при сервисном одржавању авиона. Осим CSMM-а, јављају се и друге грешке као што је *Non Performing Emitter* (NPE). Ово се односи на ситуацију када авион, иако је правилно опремљен са ADS–B Out, не емитује у складу са захтевима FAR 91.227. Међутим, FAA, у сарадњи с оператерима, тренутно ради на елиминисању грешака пилота/посаде, као што су CSMM и NPE.

ADS–B након мандата, нуди различите погодности авио-компанијама, а једно од значајних побољшања јесте проширење надзора на аеродроме и подручја у којима FAA раније није имала значајну радарску покривеност. Затим, најзначајнија оперативна предност свемирског ADS–B система је његов велики потенцијал у океанским регионима, јер овај систем може унапредити предвиђање краткорочних путања авиона. Поред тога, стручњаци сматрају да ће авиокомпаније имати значајну корист од најновијих ADS–B In апликација на одговарајуће опремљеним авионима. Најновија надоградња за ADS–B од стране RTCA *Special Committee* 186, укључује објављивање *Minimum Operational Performance Standards* (MOPS) за 1090 ES ADS–B Version 3. Ова ADS–B верзија проширује спектар доступних информација, од мониторинга, преко информација о метеоролошким условима, до ваздушне брзине, затим, побољшава предвиђања метеоролошких услова, као и друге ADS–B In апликације (нпр. *Interval Management*).

Према истраживањима и искуствима пилота као крајњих корисника, ова нова ADS–B технологија је представљена кроз бројне платформе укључене у *Electronic Flight Bag IPad*. Даље континуирано опремање авио-флота, подстиче пилоте да се

упознају са новим алатима и несметано спроводе CAVS (CDTI *Assisted Visual Separation*) током својих летова. Стечено искуство је веома важно с обзиром на то да се демонстрирају и примењују и друге апликације, као што је *Interval Management* [438]. Наиме, пилоти авиона опремљени с ADS–B In уносе одређене информације добијене од контролора летења (на пример, путању којом би авион требало да лети и ID авиона испред њих) у FIM (*Flight-deck Interval Management*) систем. Затим, FIM систем врши израчунавања, тј. даје оптимална решења, подржан инпутима из ADS–B јединице у авиону, а на FIM екрану приказује се вредност оптималне брзине лета, која омогућава безбедну удаљеност датог авиона од других испред њега, све до полетно/слетне стазе. Ова апликација омогућава пилоту бољу контролу удаљености свог авиона у односу на друге авионе опремљене ADS–B-ом, што је од посебног значаја на прометним аеродромима.

На крају, како је истакнуто [7], коришћење NextGen инфраструктуре такође ће омогућити имплементацију TBO, као и усмеравати пут прилагођавања свих операција, као што су процедуре за потпуну интеграцију UAS/дронова, свемирска лансирања, наставак истраживања у циљу смањења утицаја авијације на животну средину, повећање сајбер безбедности, итд. Поред тога, с трансформацијом инфраструктуре, FAA ће уводити нове промене. На пример, *data* комуникација такође се проширује и обухвата и лет на рути – почетне *Data Communications* (Data Comm) *En Route Services* омогућавају пилотима и контролорима размену порука, нпр. инструкције о преусмеравању, промена фреквенције за комуникацију и успостављање иницијалног контакта, док ће комплетне услуге омогућити размену података, као што су инструкције за холдинг и многе друге поруке/обавештења.

6.1.5. Ефикасност ADS–B система

ADS–B, као окосница модерног ATC, играће суштинску улогу у повећању безбедности увођењем додатног слоја надзора и ефикаснијом интер-комуникацијом између авиона и ATC. Ово ће омогућити смањење размака између авиона, ризика од судара (што је нарочито значајно у ситуацији повећане густине авио-саобраћаја), као и трошкова потрошње горива, а повећати просторну свесност ситуације. Истовремено, ADS–B доприноси побољшању квалитета животне средине, смањењем емисије гасова и буке [9–11, 18, 421, 427, 428, 439]; ADS–B је одржив извор података за глобалну транспарентну процену утицаја авијације на животну средину [21].

На основу ових ADS–B предности, произилази све већи број примена ADS–B, нарочито у системима за надзор (апликације ваздух–ваздух и ваздух–земља). ADS–B апликације могу се класификовати у различите групе [9], као нпр. *data link* апликације, ADS−B Out апликације и ADS−B In апликације [440]. До сада, стандардизација је урађена за све ADS–B Out, као и ATSAW апликације, који дистрибуирају захтеве за безбедност, перформансе и интероперабилност за различите ADS–B апликације:

- ADS–B *in Non Radar Airspace* (ADS–B NRA)
- ADS–B *in Radar Airspace* (ADS–B RAD)
- ADS–B *for Airport Surface Surveillance* (ADS–B APT)

- ATSAW *In-Trail Procedure in oceanic airspace* (ATSAW ITP)
- ATSAW *Visual Separation in Approach* (ATSAW VSA)
- ATSAW *during Flight Operations* (ATSAW AIRB)
- ATSAW *on the Airport Surface* (ATSAW SURF)
- *Flight Deck Interval Management* (ASPA–FIM)

SESAR, NextGen, EUROCAE и RTCA убрзано планирају тренутне, као и будуће активности стандардизације и регулатива, које се односе на апликације размака, раздвајања и само-раздвајања

У АТС, нови прецизни ADS–B алати, преферирани су као методе надзора у реалном времену, који помажу контролорима, јер олакшавају управљање и повећавају поузданост, безбедност и капацитет ваздушног саобраћаја [411]. Брзо преношење ADS–B података пилотима и контролорима, омогућава заједничку свесност ситуације, док ADS–B пренос података између авиона унапређује АТС оперативност у вези са одржавањем прецизних временских интервала и просторне удаљености авиона. Ове услуге обезбеђују WAM, ASSC и ASEPS:

- WAM се може инсталирати у областима где је радарска услуга недоступна/ограничена; то је земаљски систем за надзор који нуди надзор изван домета радарске покривености; побољшава ефикасност, безбедност и капацитет, јер смањује кашњења летова, број алтернација, отказивања летова и емисије штетних гасова.
- ASSC помаже у спречавању судара на полетно/слетној стази (писти) што смањује кашњења операција на Земљи.
- ASEPS као следећи ниво NextGen-а, омогућава безбедност и ефикасност у океанским *Flight Information Regions*; ADS–B подразумева и коришћење малих земаљских станица, које се једноставно одржавају и могу се поставити у областима где постављање радара није погодно/изводљиво.

У **кокпиту,** ADS–B апликације, омогућавају остваривање додатног нивоа безбедности и ефикасности, кроз доступност надзора околног саобраћаја (доступан је на свим ADS–B пријемницима), као и приступ информацијама о метеоролошким условима и лету (доступан на ADS–B In пријемницима који могу примати UAT преносе); за комерцијалне оператере, овај, потпунији надзор доприноси уштеди горива, као и времена.

ADS–B омогућене услуге у кокпиту, тј. **за пилоте**, су:

- *Automatic Dependent Surveillance – Rebroadcast* (ADS–R)
- *Traffic Information Services – Broadcast* (TIS–B)
- *Flight Information Services – Broadcast* (FIS–B)
- ADS–B *Traffic Advisory System* (ATAS)
- *Interval Management* (IM)
- CDTI – *Assisted Visual Separation*
- *In Trail Procedures* (ITP)

У кокпиту, ADS–B апликације [411], као што је поменуто, нуде већи ниво ефикасности и безбедности, као и прецизније информације. На пример, пилоти

могу користити информације о лету и метеоролошким условима (примљене путем ADS–B In пријемника), преко UAT. ADS–B омогућава услуге сервиса **TIS–B** и **FIS–B**. TIS–B повећава *situational awareness* пилота емитујући прецизне извештаје о авио-саобраћају у реалном времену, који су релевантни за авион који је опремљен у складу с прописима. FIS–B је доступан само оним авионима који могу примати податке преко 978 MHz (UAT); FIS–B емитује аеронаутичке и временске информације у реалном времену (турбуленција, залеђивање, итд.), као асистенција пилотима у ефикасном планирању безбедне путање лета, а током лета, помаже пилотима да донесу стратешке одлуке како би избегли ризичне временске услове.

ADS–B Traffic Advisory System (**ATAS**) заснован на ADS−B, веома је користан систем за мониторинг потенцијалних саобраћајних конфликтних ситуација, као и за звучна и/или визуелна упозорења. Када открије конфликт, ATAS даје звучно упозорење (саобраћајни позив), а конфликтни авиони су истакнути на екранима у кокпиту, када су такви прикази доступни. Након што прими ATAS упозорење, пилот предузима радње у складу са оперативним правилима (која су на снази). ATAS стандарди су комплетни и на располагању су произвођачима неопходне ATAS авионике. За разлику од TCAS II система, ATAS не даје савете пилотима за решавање проблема. Овај систем, ниске финансијске цене за упозоравање у генералној авијацији, смањује потенцијал ризика од судара у ваздуху [411].

Interval Management (**IM**) је ADS–B In *on-board* апликација, коју комбиновано користе летачке посаде и контролори летења за ефикасније и прецизније управљање размаком између авиона; контролори предвиђају услове саобраћаја и идентификују могућности за IM одобрења, а затим овлашћују летачку посаду за коришћење ADS–B In авионике, која обезбеђује навођење брзине за прецизно постизање и одржавање интервала размака (који издаје ATC) у односу на ″водећи″ авион. Апликације у кокпиту, као што је IM, могу дати прецизнији размак између авиона, тако унапређујући *Trajectory Based Operations* (TBO). У IM, ADS–B повећава свесност ситуације (авионика обухвата екране у пилотској кабини за приказ околног саобраћаја), дајући посади авиона правовремене препоруке за прилагођавање брзине, што омогућава одржавање потребног растојања датог авиона од других авиона. Поред омогућавања одржавања конзистентног растојања између авиона, дозвољавајући пораст протока авио-саобраћаја у доласцима, као и одржавање ефикасних путања лета у ситуацијама велике густине саобраћаја, предности коришћења IM су и смањење потрошње горива, буке и емисије штетних гасова. Авио индустрија почиње да користи ову технологију, а авио-компаније *Airbus* и *Boeing* располажу новим авионима опремљеним ADS-B In. Такође, поред сарадње са *American Airlines*-ом и ASSC-ом на сертификацији и инсталирању ADS–B In авионике у целокупну флоту *Airbus* A321 авиона *American Airlines* -а од 2022. године, FAA[183] развија захтеве за аутоматизацију и планира примену IM операције у целом NAS US након 2024. године [411].

У експлоатацији су две ADS–B In апликације: **ITP** и **CAVS** [411, 441].

[183] FAA је спонзорисала (2019) демонстрацију IM операција користећи прототип авионике, која је показала да је постизање прецизног размака (у временском интервалу 5–10 s) могуће у реалним окружењима.

ITP апликација (само за авионе опремљене с ITP) омогућава постизање, уколико је потребно, чешћих промена нивоа лета у процедуралном ваздушном простору, тако да авиони, током океанских летова, чешће лете на оптималним/мање турбулентним нивоима, смањујући ризик за кабинско особље, као и омогућавајући путницима пријатније путовање. Осим тога, предности ITP су смањење емисије штетних гасова, као и економичнија потрошња горива [148, 412]. Авиони опремљени ITP-ом имају екране у кокпиту и специјалне алгоритме који израчунавају "ITP растојање", које користе летачке посаде за утврђивање безбедне промене висине лета (пењање или спуштање). Тако, ITP-ом опремљене и обучене летачке посаде, могу захтевати ITP маневре на жељеном нивоу лета, а ATC, која сагледава укупну саобраћајну слику, може ауторизовати захтеве. Стандарди за ITP авионику су комплетни и на располагању произвођачима, а *Airbus*, *Boeing* и друге компаније нуде производе који укључују ITP функционалност.

CAVS је *Airborne Surveillance* апликација, која се користи као асистенција посади авиона за прецизније одржавање сопственог раздвајања од другог авиона (који му претходи), током узастопних процедура визуелног прилаза. Подаци претходног авиона (емитовани ADS–B Out системом), као и оног испред њега (примљени ADS–B In системом), приказују се летачкој посади на дисплеју у кокпиту (CDTI), који се може интегрисати у уобичајене навигационе дисплеје. FAA у сарадњи са *American Airlines*-ом ради на истраживању додатне употребе CAVS-а за проширење метеоролошких услова током којих се могу обављати операције које користе CAVS функционалност, у циљу повећања фреквенције слетања/полетања. Дакле, CAVS побољшава пилотову свесност ситуацији због визуелног приказа саобраћаја и смањења могућих процедура за обилазак. Очекује се да ће CAVS прикупити податке о предностима опреме ADS–B In у кокпиту.

С наставком процеса опремања авиона ADS–B In авиоником, повећаваће се и број апликација, које ће додатно унапредити све сегменте авио-сектора. У свему томе, за модернизацију глобалног ваздушног простора неопходно је да пилотске кабине задовоље оперативне захтеве у вези с иновативном технологијом, која прилагођава људске факторе до нивоа без преседана.

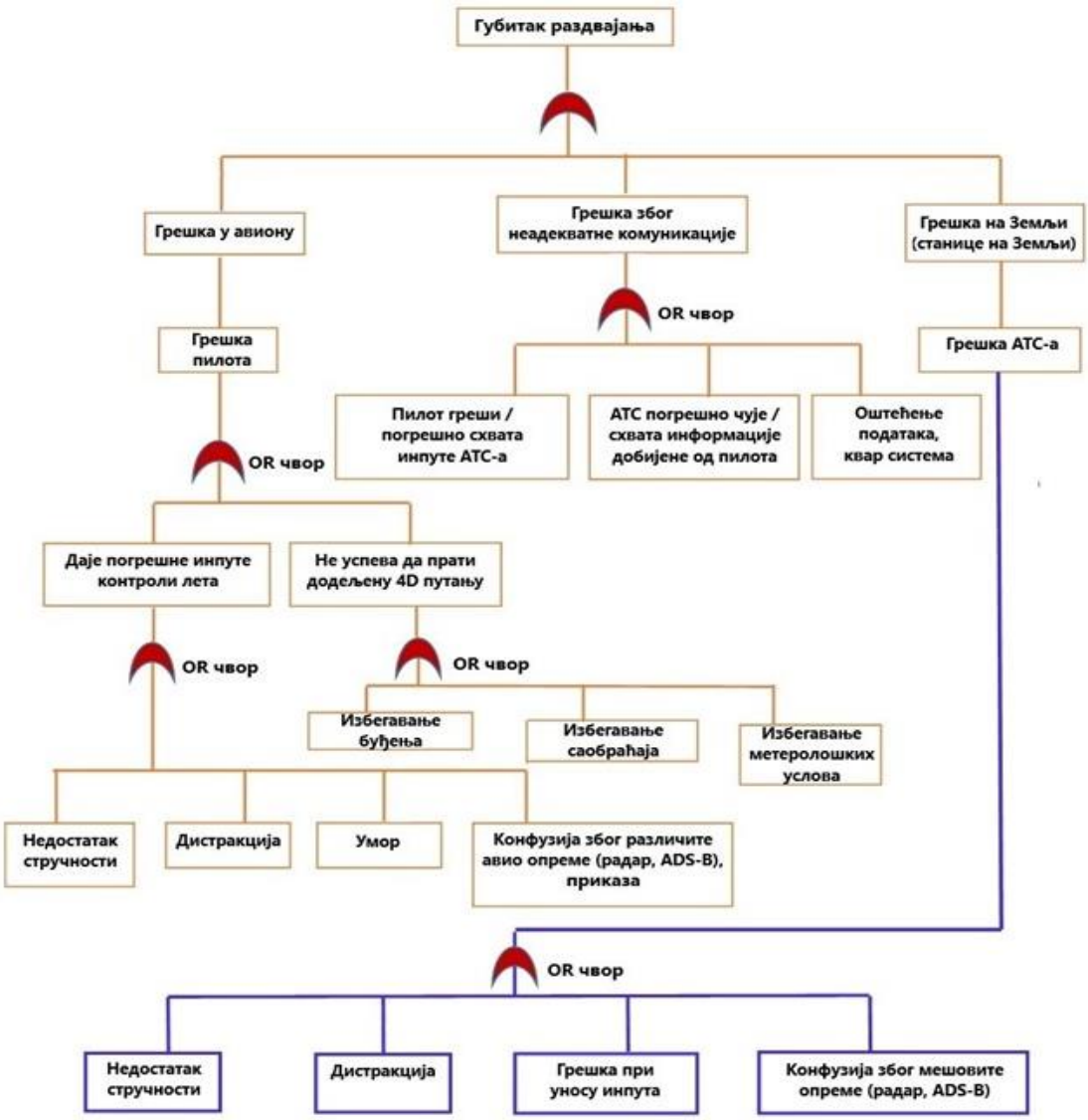
Веома важан аспект увођења ADS–B апликација јесте људски фактор, тј. интеракција људи с аутоматизованим *on-board* системима, који постају све комплекснији, а због чега од велике важности постаје и анализа безбедносних питања [442]. Анализа људског фактора, генерално, односи се на разумевање људског понашања и перформанси. Када се примењује на операције у ваздухопловству, познавање људских фактора користи се за оптимизацију интеграције људи и система које они користе или у којима раде, у циљу повећања безбедности и перформанси, тј. смањењу појаве и утицаја људске грешке у авио-системима и побољшању људских перформанси. Важно питање у вези са ADS–B технологијом је како различити корисници као што су пилоти, контролори и диспечери могу ефикасно користити информације у оквиру својих релевантних одговорности. Питања људског фактора су прихватање и коришћење ADS–B технологије од стране пилота и контролора, изградња радне етике сарадње између пилота, контролора и сертификованих органа, и начин делегирања њихове улоге и одговорности у циљу безбедног оперативног рада.

ADS–B је веома сложен систем, са специфичним компонентама ADS–B In и ADS–B Out, интегрисаних у комплетан систем, који зависи од других, спољашњих система (нпр. навигационих и комуникационих система, као и различитих система оператер/корисник). Због тога се могу идентификовати различите категорије опасности, међу којима су и оне које настају услед грешке пилота, грешке ATC и грешке која се јавља због неадекватне комуникације пилота или контролора. Постоји много могућих полазних тачака за испитивање утицаја људских фактора, а један од њих је *Fault Tree Analysis* (FTA) анализа [9]. Ова анализа, примењена на опасност од губитка раздвајања, а до које може доћи због грешке пилота (у авиону, тј. ваздуху), ATC-а или погрешне комуникације између пилота и ATC, приказана је на сл. 35. Фактори су повезани OR чворовима (логичким операторима), с обзиром на то да било који од фактора (појединачно) може довести до губитка раздвајања. На пример, фактори који доприносе грешци пилота су инпут нетачних података у ATC и немогућност праћења додељене 4D путање; ова два фактора повезана су OR чвором, јер било који од ова два фактора, може довести до губитка раздвајања.

На основу ове анализе, препорука је обезбедити релевантну обавезну обуку за пилоте, као и контролоре у вези са ADS–B технологијом, као и у погледу свесности ситуације и губитка раздвајања, затим, безбедносним аспектима у вези с комуникационим системима ваздух–земља, доношењу одлука, као и управљање ресурсима посаде. Решења су и подстицање/захтев да пилоти, као и ATC користе високо квалитетне комуникационе системе, тј. транспондере (режим C и S) и ACAS. Нарочито, требало би обезбедити и применити периодичну обуку како би се доказала њихова курентност и одредио тип рејтинга за употребу ADS–B технологије, што би значајно смањило ризике у вези с имплементацијом ADS–B система.

ADS–B систем обезбеђује податке из којих могу извести многобројне напредне апликације, као што је нпр. испитивање перформанси пилота коришћењем *Traffic Situation Awareness with Alerting Application* (TSAA) система за генералну авијацију, базираном на ADS–B-у [443]. Имплементацијом нове ADS–B опреме и процедура, повећава се број питања у вези са људским фактором, као што су разумевање употребе опреме (рад контролора и CDTI), унос и читљивост/јасноћа података, као и других људских фактора.

Како су CDTI софистициранији од друге опреме, обука пилота у вези с CDTI веома је корисна. При томе, пилоти би требало да буду упознати, много унапред, с технологијом коју користе, јер се ниво софистицираности CDTI-а мења – већина даје информације о терену, али и друге, једноставније презентације. Због тога, екран може бити с превише информација и тако комплекснији за интерпретацију, а опције постављања CDTI-а су од велике важности.



Слика 35. *Fault Tree Analysis* (FTA) анализа људских фактора ADS–B система (слика модификована и преузета из [9])

Специфичност цивилног ваздухопловства генерално, као и областима људског фактора, и нарочито у времену технолошки унапређених решења [444], односи се и на чињеницу да су ризици од замора присутни у свим сегментима рада, од оперативне припреме, преко одржавања авиона и опреме, до извршења летачких задатака. Код примене ADS–B, с аспекта људског фактора/пилота, број неких радних задатака се смањује, као што је време проведено на лоцирању одређеног саобраћаја (у случају када се користи CDTI), или време за радио-комуникационе процедуре. С друге стране, аутоматизација задатака продужава време гледања у екран, при чему је неопходна људска обрада приказаних информација на екрану. Све ово значајно повећава ментално оптерећење пилота.

Контролори морају бити упознати са ADS–B технологијом, јер, иако постоје сличности с претходно коришћеним радарским протоколима, неопходно је

разумевање процедура прилагођених ADS–B-у. Такође, и пилоти се суочавају с изазовом обраде ADS–B информација, али на другачији начин – пилоти имају додатни задатак, као што је мониторинг CDTI, којим управљају. Међутим, прецизније/тачније саобраћајне информације добијене коришћењем CDTI требало би да у великој мери побољшају пилотову свесност ситуације и значајно смање оптерећење.

Једна од заједничких перспектива и пилота и контролора о имплементацији ADS–B је одговорност. Сертификовани ауторитети и регулаторна тела морају доделити улоге и одговорности, на начин који ће допринети општој безбедности. Поред тога, следећи изазов ваздухопловне индустрије је развој ATM система који интегрише људски фактор на начин који подразумева ефикасно функционисање целог система [9].

6.2. САЈБЕР БЕЗБЕДНОСТ ADS–B АВИО СИСТЕМА

Сигурност и ефикасност, као и повећан капацитет ваздушног простора, нису једине предности ADS–B система. Увођење овог система управљања ваздушним саобраћајем следеће генерације на основу сателитске навигације, побољшава тачност, интегритет и поузданост, путем информација базираних на сателиту. ADS–B ће омогућити надзор већег броја авиона у све заузетијем ваздушном простору, без ″жртвовања″ безбедности.

ADS–B технологија омогућава смањење стандарда раздвајања, побољшава свест о ситуацији, као и има значајну улогу у побољшању квалитета животне средине смањењем емисија гасова и буке, штедећи време и гориво. С обзиром на то да омогућава пилотима да виде исте визуелне елементе који су доступни контролорима летења (друге летелице, метеоролошке услове и опасности у њиховој зони лета, као и на земљи), имплементација ADS–B повећава безбедност током полетања, слетања, као и лета. Поред тога, ADS–B проширује сателитске информације на подручја која раније нису била опслуживана радаром.

Међутим, постоје и неки недостаци, тј. рањивости (описане у делу 6.2.1), као што је зависност ADS–B система од тачности система позиционирања, односно GNSS-а, који може бити изложен ометању и лажирању (глава 5), а што може оштетити/ометати информације о позиционирању. Главна ограничења ADS–B су суштински у вези с RF комуникацијом, с обзиром на то да поруке, које се преносе у текстуалном облику, нису шифроване, нити аутентификоване. Због деликатности садржаја ових ADS–B порука, исте могу бити мета овлашћених/неовлашћених појединаца (хакера) са злонамерним намерама [2, 3]. Дакле, безбедносни ризици с којима се суочава ADS–B, односе се на везе ATC–авион, и ако оне нису безбедне, ADS–B поруке могу бити хаковане, а нарочито онда када се поруке, које садрже осетљиве информације, прекидају (*interrupt*) или прислушкују (*eavesdrop*). Поред разумевање утицаја рањивости ADS–B система на сајбер безбедност, један од циљева дисертације је и сагледавање ефикасних и ефективних метода заштите ADS–B система од сајбер напада, што је детаљно описано у поглављу 6.2.2.

Иако према FAA [411] употреба ADS–B не доводи до повећаног безбедносног ризика, показано је да, коришћењем јефтиних и комерцијално доступних хардверских и софтверских решења, нападачи могу ″ухватити″ и модификовати ADS–B поруке, избрисати их, убацити лажне (оне који доводе у заблуду) и блокирати комуникациони канал током размене података [12, 202, 445]. Поред тога, према извештају ENISA, сектор ваздухопловства је глобално изложен порасту инцидената у вези са безбедношћу информација, укључујући сајбер нападе [446] и поремећаје операција заснованих на ICT. Утицаји таквих злонамерних активности, од једноставног одвраћања пажње пилота и контролора ваздушног саобраћаја, до озбиљног ускраћивања услуга, могу, у великој мери, повећати ризик од колизије ваздухоплова и довести до деградирања безбедности националног система ваздушног простора. Према томе, неопходна су безбедносна решења за рањивости ADS–B система, а у том циљу, обим истраживања у овој области значајно се повећава [13].

6.2.1. Врсте безбедносних претњи на ADS-B систем

Унапређење комуникационих протокола употребом ваздухопловних мрежа, успостављање COTS софтверских и хардверских решења у авио-системе, затим, *Field Loadable Software* (FLS)[184], енормни пораст IoT, као и креирање концепта аутономног летења за *e-Enabled* авионе олакшали су управљање ваздушним саобраћајем уз смањење трошкова одржавања [13], али не испуњавају безбедносну компатибилност са захтеваним стандардима цивилног ваздухопловства [447]. Дакле, ова побољшања у домену комуникације, представљају безбедносни ризик, с обзиром на то да се интегритет авио система, између осталог, може деградирати активном манипулацијом података, тј. прислушкивањем, понављањем и брисањем података, као и спуфингом (поглавље 2.1.2). У овом поглављу биће разматрани (не)безбедни аспекти RFI у авијацији, и то нарочито ADS–B система.

Дакле, питање које следи је: да ли би злонамерне ADS-B поруке могле збунити пилоте, или контролоре летења, и тако довести до опасних ситуација?

Како ADS–B подржава аутоматске критичне задатке и људске одлуке, и има директан утицај на укупну безбедност ваздушног саобраћаја, императив је да ADS–B технологија, осим оперативних и захтеваних перформанси, испуни и захтеве у вези са сајбер безбедношћу. Међутим, суштински проблем ADS–B система је недостатак сигурносних механизама, и то недостатак [12]:

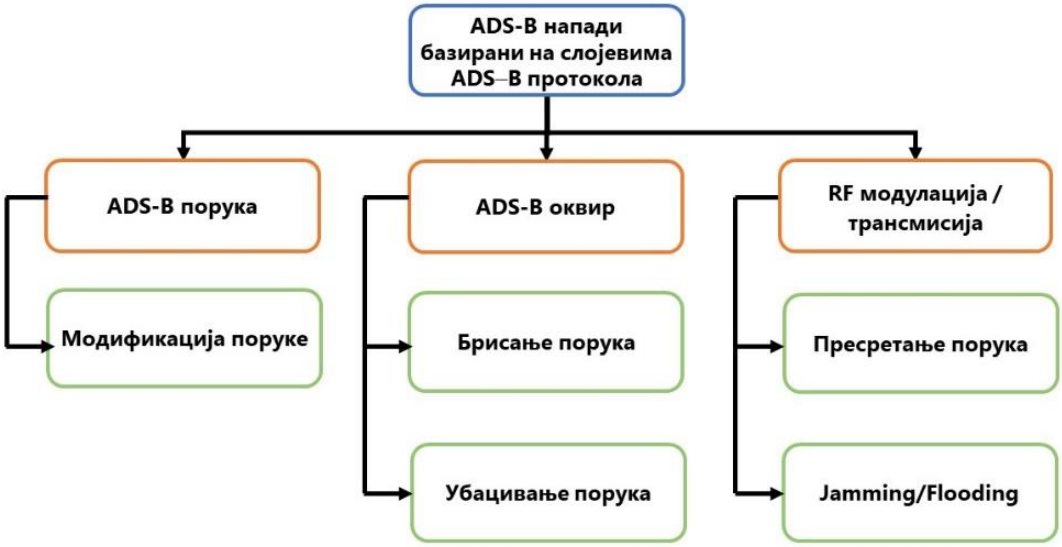
- аутентификације ентитета у циљу заштите од убацивања порука од стране неовлашћених субјеката
- потписа порука/кодова за потврду аутентичности, за заштититу од неовлашћеног мењања порука или лажног представљања авиона
- енкрипције порука за заштиту од прислушкивања
- механизама изазов-одговор за заштиту од напада понављања

[184] FLS је систем, који испоручује сигуран софтвер за авио-компоненте преко мреже одобрених сервисних станица произвођача у циљу подршке безбедним и ефикасним операцијама генералне авијације.

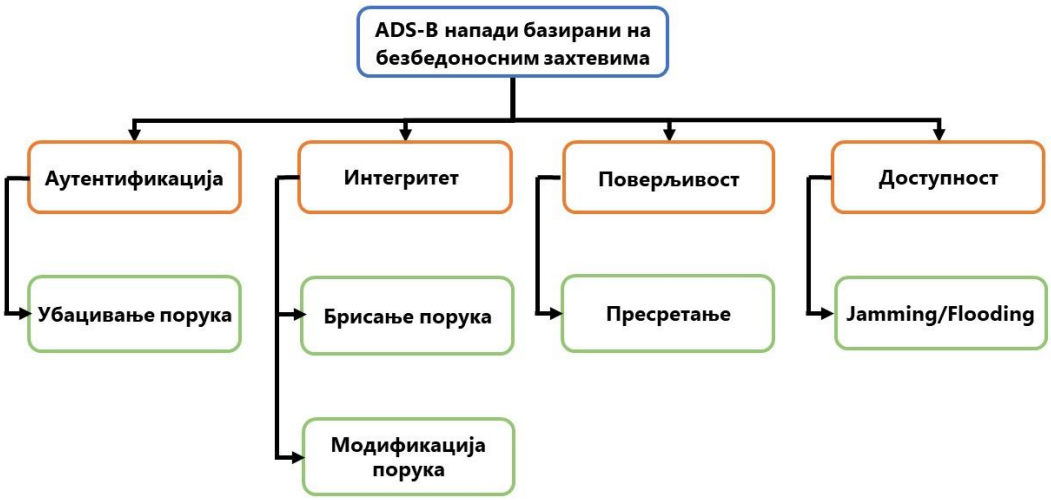
- ефемерних идентификатора за заштиту од напада праћења

Дакле, због ових ограничења, могуће су различите врсте сајбер напада на ADS–B систем [448]. Могу се успоставити две различите **класификације сајбер напада** на ADS–B: једна заснована на слојевима ADS–B протокола који се компромитују, и друга заснована на ADS–B безбедносним захтевима (сл. 36а и б) [13].

(а)



(б)



Слика 36. Класификација ADS–B напада према слојевима ADS-B протокола које компромитује (а) и безбедносних захтева (б) (модификовано и преузето из [13])

На пример, модификација поруке (сл. 36а), компромитује функцију формирања поруке ADS–B протокола, док брисање и убацивање порука, компромитују подслој оквира ADS–B протокола, с обзиром на то да ови напади додају/уклањају поруке

из ADS–B оквира који се преноси. Напади прислушкивања и ометања најчешће се предузимају на физичком нивоу, тако да се ови напади класификују у RF модулације ADS–B протокола.

С друге стране, класификација сајбер напада према безбедносним захтевима, дата је на сл. 36 (б). Ови **безбедносни захтеви** обухватају:

- Аутентификацију – могућност комуникационог пријемника да у сваком тренутку идентификује авио-предајника; ињектирањем порука у комуникације легитимних ентитета, злонамерни комуникациони чвор може емитовати ADS–B поруке користећи лажне идентитете који се не могу потврдити.
- Интегритет – захтева непроменљивост ADS–B порука током преноса, тако да се напади брисањем и модификацијом порука сврставају у ову категорију.
- Поверљивост – доступност података на мрежи искључиво овлашћеним субјектима; свака активност која доводе до ″цурења″ информација неовлашћеним или злонамерним корисницима, угрожава поверљивост, тако да се напад прислушкивањем сврстава у ову категорију напада.
- Доступност – доступност ADS–B порука и услуга овлашћеним/потписаним субјектима; нпр. нападач може једноставно ометати земаљску ADS-B и извршити напад ускраћивања услуге, тако да се ометање/*flooding* класификују у ову категорију.

Табела 9. Врсте, мотиви и начини сајбер напада на ADS–B систем [427]

Врста напада	Мотив напада	Начин напада
Прислушкивање	Прислушкивање информација о радном статусу ваздухоплова (извиђање)	Пресретање/добијање ADS-B података од ADS-B In
Ометање	Ометање преноса ADS–B поруке у одређеном ваздушном простору	Коришћењем ADS-B предајника велике снаге у одговарајућем опсегу фреквенција
Убацивање порука	Убацивање лажног ваздухоплова у специфични сценарио лета, доводећи до конфузије ATC система	Коришћењем одашиљача велике снаге преноса у релевантном опсегу фреквенција и с могућношћу коректне модулације и потврде формата ADS-B поруке
Брисање порука	Брисање неких/свих информација садржаних у поруци (нестанак авиона)	Конструктивна или деструктивна интерференција, које се имплементирају на физички слој система
Модификација порука	Промене информација садржаних у поруци (модификација виртуелне путање)	Сенчење и бит-флипинг на систему (физички слој) или комбинацијом различитих врста напада (убацивање лажних порука и брисање порука)

Напади на ADS–B, могу имати различит ниво утицаја (штетног) на авио системе, и обухватају **прислушкивање**, **ометање**, **убацивање порука**, **брисање порука** и **модификацију порука** (табела 9) [18, 449]; ови напади биће детаљније објашњени у делу 6.2.1.1. Тако, прислушкивање проузрокује минималну штету и не оштећује директно ATC систем, док брисање порука утиче на систем надзора ваздухоплова, који привремено нестаје са ATC мапе, али се, у овом случају,

ваздухоплов може идентификовати радаром или мултилатерационим системом. Модификација порука јесте типичан спуфинг напад, тј. напад лажирања и има велики утицај на АТС систем. На пример, суфинг напад, назван "кувана жаба" [450], односи се на ситуацију у којој нападач континуирано, али у малој мери, мења информације о позицији ваздухоплова у ADS–B порукама. У овом случају, технологије надзора, нпр. системи радарског надзора, као и позиционирања, тешко детектују мале разлике, које су у оквиру тачности подешавања, што резултира у непрецизном вођењу ваздухоплова од стране АТС као и закаснелог (одложеног) одговора система за спречавање колизије у ваздуху.

6.2.1.1. Радио-фреквенцијске интерференције (RFI)

Рањивости ADS–B система суштински потичу од природе бежичног протокола ADS–B и чињенице да ADS–B систем емитује поруке као нешифровани отворени текст. Због недостатка безбедносних процедура за пренос ADS–B података, као и широке доступности SDR (фуснота 136), малициозни хакер може нпр. модификовати ADS–B поруке у циљу виртуелне модификације путање авиона, брисати ADS–B поруке, као и симулирати непостојећи авион (″авион-дух″) на екранима АТС. Ове рањивости ADS–B изазивају забринутост, нарочито с обзиром на неопходност потпуне усклађености од стране ваздухопловне индустрије, због чега се и бројне, најскорије објављене публикације баве питањима сајбер напада на ADS–B систем [13, 14, 18, 19, 448, 451–457].

Нападач може извршити различите врсте сајбер напада на ADS–B, као што су:

- прислушкивање, тј. пресретање поруке (*eavesdropping, i.e. message interception*)
- ометање (*jamming*), тзв. *flooding*
- брисање поруке (*message deletion*)
- убацивање поруке (*message injection*)
- модификацију поруке (*message modification*).

Прислушкивање (пресретање порука) је најједноставнији и најдиректнији безбедносни пропуст ADS–B због недостатка енкрипције, и односи се на пасивно праћење емитованих преноса/комуникације. Иако постоји неколико сервиса који легално користе ову функцију за праћење ваздушног саобраћаја, прислушкивање представља ризик, јер се може користити за покретање софистициранијих напада (комбиновањем ADS–B података и других јавно доступних података, из нпр. званичних база података које обезбеђују ваздухопловне власти) [426]. Такође, због недовољне енкрипције порука, технички је немогуће избећи овај облик RF интерференција, а техничке реалности узрокују и да закони против ових активности, донети у неким државама (нпр. UK), буду неефикасни.

Ометања (*jamming*) је активни напад (сложенији од прислушкивања) у коме хакер намерно шаље IP пакете у циљу ометања слања/примања података од стране аутентичних учесника у комуникацији, што касније резултира ускраћивањем услуге. Ометач, континуираним слањем пакета података, може проузроковати да аутентични корисник никада не детектује неактиван канал. Ометање је озбиљан проблем у бежичним мрежама, а у ваздухопловству нарочито, с обзиром на

критичност података, као и на широк и отворени оперативни простор без контроле. За извођење напада ометања, ефикасним блокирањем комуникационих канала, примењују се два приступа, и то: *Ground Station Flood Denial* и *Aircraft Flood Denial*. Циљ обе врсте напада је поремећај фреквенције комуникације и прекид мреже за надзор. Извођење прве врсте напада је једноставније, јер захтева сигнале ометања мање снаге, с обзиром на то се нападач може наћи у непосредној околини мете. Иако може довести до губитка система за надзор, овај напад је локализован, у зависности од снаге сигнала на одређену (једну) област, тако да има средњи до висок ризик на АТС.

Убацивање поруке (*message injection*) омогућено је услед непостојања провере аутентичности *data link* слоја ADS–B мреже, и може се извести коришћењем једноставних и комерцијално доступних технологија [12, 445]. Слично претходно поменутом нападу, напади убацивањем псеудо-легитимних порука, могу бити *Ground Station Target Ghost Injection* и *Aircraft Target Ghost Injection* [413]. На пример, у првом нападу, нападач креира и емитује лажне ADS–B поруке, које су истих карактеристика као и легитимне ADS–B поруке, тако да се не може направити разлика између њих. Као и код напада ометања, напади убацивањем порука, у оба случаја (циљ је мета на земљи или мета у ваздуху) проузрокује појаву нелегитимних мета духова, који се појављују као валидни чворови мреже. У зависности од циља напада, исти може имати средњи или високи ниво ризика на авио-сектор. Тако, уколико се напад изводи у циљу одвраћања пажње пилота и контролора, има средњи ниво ризика и малог је утицаја на авио-сектор. Међутим, уколико је број лажних ADS–B порука велики, напад убацивањем порука, може деградирати систем за избегавање судара и тако значајно угрозити функционисање ваздушног саобраћаја. У овом случају, напад убацивањем порука представља висок ризик за АТС.

Брисање поруке је сајбер напад који се заснива на брисању ADS–B легитимних порука са ADS–B мреже. Пример је напад нестанка авиона, који се може извести коришћењем конструктивне или деструктивне интерференције. У првој методи, нападач изазива довољан број значајних грешака у ADS–B поруци, тако да је прималац сматра оштећеном, и исту одбацује. Наиме, ADS–B комуникациони протокол (део 6.1.2) обухвата 24-битни сегмент, који укључује проверу паритета и може исправити до 5 битова грешака по поруци; свака порука са више од 5 битова грешака сматра се оштећеном и одбацује се. У методи деструктивне интерференције, нападач уништава легитимни ADS–B сигнал, тако што благовремено генерише синхронизовани, инверзни ADS–B сигнал, чиме се на једноставан начин смањује или уништава (делимично/употпуности) легитимна ADS–B порука. Како је за извођење напада кључна временска синхронизација, ова врста напада је теже изводљива и мање ефикасна. Исход обе врсте напада је да легитимни ваздухоплов постаје невидљив за друге авионе и беспилотне летелице, што може довести до поремећаја ваздушног саобраћаја и повећаног ризика од судара авиона. Брисање ADS–B порука, представља ризик средње јачине, јер има малу вероватноћу извођења (због комплексности и неопходне временске синхронизације); чак и уколико, услед овог напада, авион постане невидљив

контролорима, систем за надзор подржан је резервним системом, као што је MLAT, што смањује ризик од ове врсте напада.

Модификација порука легитимних чворова у мрежи, најтеже је изводљива врста напада у односу на друге [451], јер нападач мора имати приступ легитимном мрежном комуникационом хардверу током преноса поруке, што је много теже остварљиво. Нападач користи два различита приступа за модификацију поруке, и то сенчење/затамљење (*overshadowing*) поруке и инверзију битова (бит флипинг, *bit flipping*). У првом приступу, нападач користи сигнале велике снаге, који су прецизно усклађени с преносом циљане поруке, у сврху њене потпуне/делимичне замене/модификације; код ове методе, за разлику од ометања, мета нападача је одређени комуникациони чвор, а није цео комуникациони канал. У другом, *bit flipping* приступу, нападач конвертује било који број битова од 1 до 0 (или обрнуто) преклапањем лажног сигнала преко оригиналног. У оба приступа, произвољни подаци могу бити убачени у мрежу, без знања легитимних учесника. Модификација порука може се извести и комбиновано, брисањем и убацивањем поруке, што резултује појавом нове модификоване поруке на мрежи. Међутим, у односу на овај приступ (убацивање потпуно нове поруке), прва два приступа (модификација порука на нивоу ADS–B комуникационог хардвера), много су проблематичнија, јер се легитимна порука модификује у току преноса, тако да их примаоци сматрају легитимним [451, 458, 459]. Напад модификације поруке има велики утицај на ATC, јер нападач може даљински отети авион/изазвати авионске несреће. Међутим, вероватноћа овог напада је минимална, због комплексности извођења напада (неопходна прецизна временска синхронизација), тако да овај напада припада онима који су средњег до високог ризика.

Модификација поруке јесте типичан **спуфинг напад** (*spoofing attack*). Као што је детаљно дато у делу 5.2.1.1, спуфинг напад, тј. напад лажирањем, један је од облика намерних RFI и може се анализирати или као посебан облик напада, или као потпуно засебна категорија напада. Ипак, не може се успоставити оштра граница између спуфинга и RFI, тј. где се завршава једна, односно почиње друга врста напада, јер неки спуфинг напади могу довести до престанка рада GNSS пријемника, иако нема RF преоптерећења. С обзиром на велики (штетан) и опасан утицај који може имати на ATC систем, спуфинг напад ће бити детаљније објашњен у наставку текста.

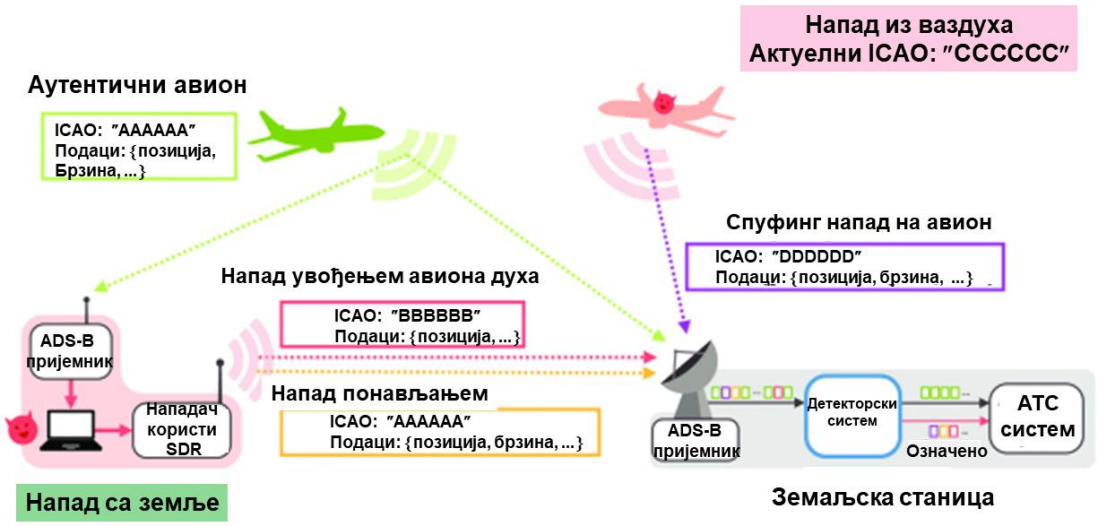
Спугинг напад остварује се модификацијом ADS–B порука, убацивањем лажних/фалсификованих порука. Може се класификовати у две категорије, и то: спуфинг напад са Земље и спуфинг напад из ваздуха [19]. Различите врсте спуфинг напада, и то спуфинг напад убацивањем порука и спуфинг напад на земаљску станицу, илустровани су на сл. 37.

У првој врсти напада (напад са Земље), нападач користи јефтини SDR за:

- ре-емитовање претходно снимљене поруке (тзв. напади понављањем, тј. репродукцијом IQ података[185]), или

[185] IQ подаци (сигнали, узорци или квадратурни сигнали) – периодични сигнали, чија је фазна разлика 90^0; слова I и Q, односе се на *in*-фазу (референтни сигнал) и фазно померени сигнал, редом.

- пренос ново-генерисане, коректно модулисане лажне поруке (напад увођењем авиона ″духа″)



Слика 37. Илустрација различитих врста спуфинг напада на ADS-B: напад са Земље (коришћењем SDR спуфера) и напад из ваздуха, тј. авиона (нападач користи ADS–B транспондер с измењеном ICAO адресом (модификовано и преузето из [19])

У нападу репродукцијом IQ података, **нападач са Земље**, користећи SDR уређај, снима садржај порука/IQ податке примљених аутентичних ADS–B порука, након чега их емитује с кашњењем, али без промене њиховог садржаја. Овај напад је веома софистициран, с обзиром на то да IQ подаци садрже важне информације, као што су оне у вези са Доплеровим ефектом, карактеристикама предајника и особинама комуникационих канала. У другој врсти напада, тј. нападу увођењем авиона ″духа″, нападач са Земље, користећи SDR уређај, емитује лажне ADS–B поруке произвољног садржаја. Нарочито, нападач може симулирати путање непостојећих ваздухоплова, тј. ваздухоплова ″духова″, и генерисати одговарајуће ADS–B поруке пажљивим избором Доплерових помераја, и тако учинити да ови авиони–духови постану видљиви станицама на Земљи.

У другој врсти напада, тј. **нападу из ваздуха** (спуфинг авиона), нападач, користећи ADS–B транспондер у ваздуху, модификује ICAO адресу у ADS–B порукама, представљајући се као познати/поуздани авион, тако заобилазећи надзор. Тако, нападач с авионом (злонамерни авион) покушава да се маскира у познати/поуздани авион, лажирањем ICAO адресе и прикривањем свог стварног идентитета. Због физичког присуства авиона, овај напад не може се детектовати, чак ни од стране секундарног радара за надзор (SSR).

За разлику од напада на ADS–B система, који се изводи са земље, потенцијални напади, а који би се могли остварити из ваздуха, недовољно су анализирани [12], али представљају реалну претњу. Ови напади могу се реализовати коришћењем

UAS/дронова, а узимајући у обзир константан техничко-технолошки напредак, на ову врсту потенцијалног сајбер напада требало би обратити нарочиту пажњу. Због тога, истраживачки пројекат *OpenSky Network* прикупља извештаје у вези са ADS–B, и омогућава доступност података за безбедносне/сигурносне анализе, затим, развој концепција детекције спуфинга, као и лоцирања спуфинг уређаја/извора.

Поређењем различитих врста сајбер напада на ADS–B [13, 149], сматра се да је вероватноћа извођења напада прислушкивања[186] највећа (због недостатка безбедносних алгоритама и стандардизованог ADS–B протокола, ниске цене ADS–B пријемника и коришћених фреквенција), а најмања спуфинг напада. Међутим, безбедносни ризик спуфинга веома је висок (у спуфингу, нападач може убацити, обрисати или изменити садржај ADS–B поруке), док је рањивост авио-система од прислушкивање најмања.

На крају, сајбер безбедносни ризик по ADS–B, је већи него ризик за традиционални радарски систем (SSR), због недостатка безбедносних алгоритама, као и ниске цене ADS–B пријемника [149]. Поред тога, ADS–B *on-board* транспондер периодично емитује информације пријемницима на Земљи, омнидирекционално, за разлику од SSR, који усмерено испитује *on-board* транспондере, који имају велику снагу преноса. Такође, ADS–B пријемници су једноставнији у поређењу са механичким ротирајућим антенама, које се користи у SSR.

Рањивости ADS–B система, као што је претходно објашњено, првенствено потичу од нешифрованог и неауторизованог бежичног преноса порука између авиона и станица на Земљи. Нападачи који су у домету ADS–B преноса, могу безбедносно угрозити функционисање ATC. Ови нападачи могу се класификовати према улози/месту нападача у систему, његове физичке позиције, као и циљу напада [12]. Тако, према месту које нападач има у систему, категоризација обухвата следеће врсте нападача [202]:

- Инсајдери – особе са злонамерним намерама (особље аеродрома, земаљских станица или чланови посаде авиона). Чињеница да је велики број особа које имају овлашћење физичког приступа ограниченим областима, као и IT системима и међусобно повезаним уређајима и мрежама, повећава ризик од извођења сајбер напада. Нарочито, уколико је мета напада авион у ваздуху, успешност напада је већа, уколико га предузима злонамерни инсајдер него удањени (екстерни) нападач.
- Злонамерни путници на аеродромима/у авионима – нападачи који имају ограничен приступ физичким површинама и опреми, тако да је ризик од успешног напада који они предузимају, мањи од инсајдерског напада. Иако мање вероватан, злонамерни путник у авиону може предузети различите врсте ADS–B напада на авион током лета.

[186] У нападу прислушкивања, нападач само прима бежични сигнал, док у нападу ометањем, нападач трансмитује бежични сигнал у циљу блокирања ADS–B сигнала.

- Удаљени нападачи – нису физички присутни на аеродрому или у авиону, немају приступ ADS–B системима и најчешће предузимају сајбер нападе с непознатих локација. Област њиховог напада је ограничена, а мета мора бити у домету напада. Међутим, удаљени нападачи могу ефикасно извршити нападе ускраћивања услуге и угрозити ATC у подручју с њиховом покривеношћу. Вероватноћа присуства ових нападача је већа од инсајдер нападача и злонамерних путника.

Сајбер напади на ADS–B систем могу утицати на поузданост комуникације између авиона и ATC, што у коначном, може угрозити читав оперативни систем управљања услед достављања непоузданих података другим информационим системима. Тако, компромитовани систем може имати каскадни ефекат на укупно функционисање ATC. Системи и поступци који могу утицати на укупан рад ATC су [202]: Системи за комуникацију, навигацију и надзор (*Communication, navigation and surveillance systems*); ATC навигациона средства и приступи (*Air traffic management navigational aids and approach*); Системи за праћење лета (*Flight tracking systems*); Систем приказа лета и управљање (*Flight display system and management*); Системи контроле одласка (*Departure control systems*); Центар за надзор и контролу система (*System monitoring & control center*); Комуникациони систем путник-авиокомпанија (*Passenger-airline communication system*).

6.2.2. Заштита ADS–B од сајбер напада: безбедносна решења

Један од циљева дисертације јесте процена утицаја рањивости ADS–B, авио-система који се ослања на технологију сателитског позиционирања, а који може бити мета различитих врста сајбер напада (поглавље 6.2.1), међу којима забринутост и нарочиту пажњу изазива спуфинг, идентификован као много опаснији облик сајбер напада у односу на намерно ометање – у спуфингу се у пријемник "жртве" убацују/подмећу лажни сигнали, тако да циљани пријемник не може открити напад, нити упозорити корисника на непоуздана навигациона решења. Штавише, и ако није у потпуности успешан, спуфинг ињектира штетне информације и узрокује значајне PVT грешке. Иако је спуфинг у цивилној авијацији потенцијална претња, као што је дато у поглављу 6.2.1, његова техничка изводљивост је реална, а примена постаје флексибилнија [335]. Нарочито, реалан и веома велики ризик представљају потенцијални напади који би се могли остварити из ваздуха, употребом UAS/дронова у циљу отмице или дистрикције безбедности у надзору ваздушног простора.

Ипак, авијација није безочно изложена спуфингу и осталим врстама сајбер напада, без икакве одбране. Наиме, применом одређених метода, ови сајбер напади могу бити ублажени. Поред тога, и пилоти су оспособљени да детектују и решавају проблеме у свакој фази лета. Свакако, због могућих софистициранијих врста сајбер напада, међународне организације, као што су ICAO и EUROCAE, проактивно се баве повећањем робустности ADS–B система на сајбер нападе, а међу њима и спуфингом. С обзиром на значај теме и чињеницу да тестирање метода за ублажавање и детекцију сајбер напада подразумева разматрање специфичности и могућих сценарија одређене врсте напада, у наставку текста биће дат краћи преглед

најновијих истраживања у вези са против-мерама и техникама за ублажавање рањивости ADS–B система у цивилној авијацији.

Током протекле деценије, у многим истраживачким радовима веома важна тема била је безбедност протокола емитовања у бежичним сензорским мрежама, као и налажење решења за повећање безбедности ADS–B система. У циљу заштите бежичне ADS–B комуникације, потребно је уградити механизме и против-мере које би тестирале интегритет као и веродостојност примљених ADS–B порука. У том смислу, предложени су бројни безбедносни механизми, а безбедносна решења се могу класификовати у две групе, и то [13, 451]:

- Безебедносне технике засноване на **аутентификацији емитовања/поруке** – обухвата технике (криптографске и некриптографске) које осигуравају интегритет поруке, тј. обезбеђују протокол аутентификације поруке и потврду примаоцу да су примљене поруке стигле од аутентичног извора, као и да нису пресретнуте/промењене током преноса.
- Безбедносне технике засноване на **верификацији локације** – ове технике заснивају се на идентификацији и верификацији локације корисника ADS–B мреже. Обухвата верификација у региону и безбедно одређивање локације. Првом методом се покушава утврдити кредибилитет тражене локације у примљеној ADS–B поруци коришћењем алгоритама за одређивање вероватноће са којом се одређује тачност позиције. Другом техником директно се идентификује физички положај авиона у циљу унакрсне провере кредибилитета локације; информације о локацији, могу користити и ADS–B и радар, у алтернацији, уколико неки од ова два система не функционише.

У овом делу, укратко ће бити описане постојеће технике за ублажавање сајбер рањивости ADS–B система. Детаљна анализа ADS–B напада, контра-мера и њихових предности/недостатака, као и проблема имплементације могу се наћи у прегледним радовима [13, 337, 338, 460]. Такође, категоризација и описи могућих спуфинг напада, детаљно дати у радовима [337, 338], омогућавају дефинисање различитих сценарија за тестирање перформанси предложених анти-спуфинг техника у авијацији [333]. Безбедносне технике засноване на аутентификацију емитовања/порука, као што је поменуто, могу се поделити на **криптографске** и **некриптографске** технике.

Криптографске технике за аутентификацију поруке, обухватају симетричне и асиметричне технике (*Public Key Infrastructure, Timed Efficient Stream Loss tolerant Authentication, Message Autentification Crypto*, итд.) и захтевају модификације постојећег ADS–B протокола, што их измешта у област безбедног пројектовања и модуларних техника за дистрибуцију и управљање, због чега се ове технике веома тешко имплементирају [461, 462]. Такође, криптографска решења која повећавају дужину ADS–B поруке, повећавају и сметње на каналу, као и доводе до ограничености капацитета, а свако од решења мора бити глобално одобрено од стране ваздухопловних ауторитета.

Техника *Public Key Infrastructure* (PKI) заснива се на приступу асиметричног кључа. У приступу конвенционалног асиметричног кључа, ауторитет за сертификате, најпре верификује сваки ентитет у мрежи, и додељује му јединствени

пар јавно-приватног кључа (познатог свим верификованим чворовима у мрежи, док је приватни кључ специфичан за сваког корисника). На овај начин, само легитимни чворови у мрежи могу остварити комуникацију. У PKI, сваки пошиљалац шифрује поруку јавним кључем пријемника; шифровану поруку може дешифровати само приватни кључ датог пријемника. Ово обезбеђује интегритет података, јер ниједан други пријемник, осим предвиђеног, не може дешифровати поруку. Дакле, PKI се заснива на приступу асиметричног кључа прилагођеног за ADS–B: чвор *X* шаље свој дигитални потпис путем *m* порука, тако да чворови у околини примају *X*-ов дигитални потпис након сваких *m* порука. Када чворови из околине приме цео дигитални потпис, они могу проверити аутентичност порука у баферу. Дистрибуција PKI кључева може се извршити током циклуса планираног одржавања авиона [451].

Адаптација конвенционалне асиметричне криптографије је и *Timed Efficient Stream Loss-Tolerant Authentication* (TESLA)[187] [463], у којој предајници шаљу своје кључеве ретроактивно, а које затим користе примаоци за аутентификацију емитованих порука. Чвор за емитовање генерише кôд за аутентификацију поруке (MAC), шифрује га и додаје свакој поруци. Након одређеног временског периода/броја порука, објављује се кључ за дешифровање MAC-а пошиљаоца. Стога, примаоци који су прикупили емитоване поруке могу дешифровати поруке. Као безбедносно решење за ADS–B, TESLA обезбеђује интегритет порука, али уводи кашњење у емитовању порука, због неопходности њиховог баферовања.

С друге стране, **некриптографске технике** безбедности мрежа заобилазе проблем дистрибуције кључева, и обухватају приступ **″отиска прста″ физичког слоја** и технологију **проширеног спектра** (фреквенцијске модулације). Методе отиска прста укључују неколико приступа за аутентификацију и идентификацију јединствених карактеристика аутентичних мрежних чворова (преко хардверских или софтверских несавршености или преко карактеристика фреквенције канала). Приступи засновани на софтверу настоје да идентификују јединствене карактеристике софтвера, док оне засноване на хардверу покушавају да категоризују и препознају различитости мрежног хардвера (за препознатљивост јединствености уређаја може се користити нпр. разлика у модулацији радио сигнала или синхронизација часовника). Техника проширеног спектра, користи се у бежичној комуникацији као против-мера ометању и прислушкивању. За имплементирање методе, неопходно је да предајник и пријемник имају приступ унапред дељеном кôду за ширење (техника директне секвенције проширеног спектра) и шаблону прескока (техника фреквенцијског прескока проширеног спектра), због чега је неопходно имати приступ или информације о кôду за ширење/образац прескока за праћење или прислушкивати комуникације у циљу блокирања канала. Недостатак је, слично криптографским техникама, дистрибуција кôда и управљања у систему (и пошиљалац и прималац морају пратити унапред дефинисани кôд или образац). Поред тога, техника ширења спектра није

[187] Постоји и варијација TESLA технике, названа μTESLA протокол, који користи шифровање асиметричним кључем преко одложеног откривања симетричних кључева, што доводи до ефикасне технике за уградњу у ADS–B.

компатибилна с ADS–B инфраструктуром и захтева значајне модификације система.

Други безбедносни приступ, тј. безбедне технике засноване на **верификацији локације**, за разлику од првог приступа, настоје да идентификују, као и верификују локације, које су декларисане од стране ентитета ADS–B мреже [13]. Овај приступ обухвата различите технике [451] као што су: ограничавање удаљености (*distance bounding*), Калманово филтрирање, мултилатерација (MLAT), фузија података, итд.

Ограничавање удаљености (*Distance Bounding*) је метода верификације локације у региону, која се базира на додатном делу информације о удаљености (рачуна се из времена повратка сигнала, односно пређеног пута поруке од верификационог до доказног чвора и брзине светлости, коме се додаје одређено времена обраде), који се користити за верификацију исправности тражене локације чвора. Штавише, трилатерацијом и ограничавањем удаљености, може се идентификовати реална позиција чвора. Међутим, ова техника није адекватна за покретне чворове/објекте велике брзине, тј. ADS–B, и може бити мета различите врсте напада, као што су отмице или напади преваре. Пред тога, техника захтева значајну промену ADS–B протокола, јер се базира на двосмерном комуникационом протоколу, тј. побуду верификатора и одговор на побуду.

Калманово филтрирање (*Kalman Filtering*) или линеарна квадратна процена [464] базира се на анализи серије мерења која садрже шум и процењивању непознате променљиве. Алгоритам се састоји од три процеса: предикција (предвиђају се променљива стања система као и повезане неизвесности, које зависе од тренутног стања система, прелазног стања из претходног у тренутно стање, као и улаза у систем), посматрања (алгоритам модификује вредности процене рачунајући грешку изражену као разлика између мерења тренутног посматраног стања и пројектованих мерења израчунатих у претходном кораку) и ажурирања (процене се ажурирају и пондеришу, а проценама с већом вероватноћом се додељују веће статистичке тежине). Ова три процеса чине повратну контролу у којој филтер процењује стања система у било ком тренутку, а затим добија повратну информацију, чиме се побољшава процена резултата. Калманово филтрирање се већ користи у АТС за филтрирање GPS сигнала (део 5.3.1.1.), као и за избегавање судара авиона на полетно/слетним стазама и рулним стазама. Има и веома важну улогу у методи мултилатерације, тако што уклања шум примљеног сигнала, а нарочито се користи за проверу аутентичности примљених података из авиона опремљеног ADS–B-ом [465]. Калманово филтрирање има неколико актуелних и потенцијалних апликација за АТС, али има и рањивости, и то, суфинг напад, назван "кувана жаба", у коме, као што је претходно поменуто (део 6.1.1.) нападач омета сигнал аутентичног чвора и убацује лажне податке о локацији малом брзином, тако да Калманов филтер не региструје промену сигнала. Поред тога, како Калманово филтрирање захтева више времена за обраду података и комплексније рачунарске системе, рањиво је и на нападе ускраћивања услуге [451].

Трилатерација (*Trilateration*) и мултилатерација (*Multilateration*) су технике процене положаја, које се базирају на мерењу удаљености између циљане тачке (предајника) и скупа референтних чворова (пријемника), употребом система временске пропагације, као што је *Time of Arrival* (ToA) или *Time Difference of*

Arrival (TDoA). У ToA [466], удаљеност између сваког пријемника и предајника, јесте производ ToA и брзине путовања сигнала[188]. За повећање тачности и ефикасности, користи се мултилатерација помоћу TDoA или хиперболичке локализације. То је техника у којој се положај (тро-димензионални, 3D) процењује на основу временске разлике доласка сигнала од извора до четири/или више позната чвора (пријемника) који су повезани с центром за обраду, тако да није потребна синхронизација између извора и пријемника, осим временске синхронизације пријемника. TDoA локализација се користи за позиционирање авиона на земљи на различитим америчким аеродромима [467], а главна предност технике је то што не захтева никакве модификације у авиону. Као проширење мултилатерације, мултилатерација широког подручја (*Wide Area Multilateration*, WAMLAT) такође се користи у циљу одређивања локације ваздухоплова. WAMLAT је економичнија и једноставнија техника за имплементацију у поређењу са примарним радарима за надзор. Међутим, у удаљеним областима као што су океани, имплементација WAMLAT-а није изводљива, што је један од разлога развоја мултилатерације коришћењем ADS–B сигнала. Тако, имплементација хибридног механизма (нови комуникациони систем ваздух–земља заснован на адаптивној модулацији и обради сигнала техником просторног филтрирања, коришћењем ADS–B и техника мултилатерације) омогућава прецизна одређивања локације авиона [468]. Међутим, имплементација мултилатерације повезана је са одређеним проблемима, као што су безбедносни, као и са тачним израчунавањем TDoA. Такође, тачност одређивања положаја зависи од бројних пријемних станица, тако да квар на било којој земаљској станици, може компромитовати ова одређивања.

Групна верификација (*Group Verification*) је метод утврђивања безбедне локације ADS–B, који користи поуздана група авиона (четири и више) који обављају мултилатерацију у ваздуху [469]. Да би постали чланови групе, авиони би требало да потврде аутентичност, а затим применом мултилатерације, идентификују позиције оних који нису чланови групе у ваздуху. Када се идентификује лажна позиција, авиони повећавају своју безбедну удањеност и даље поступају у складу са ситуацијом. За примену групне верификације, неопходно је да сваки авион буде опремљен с ADS–B In, а како је ово опциони модул, потребна су додатна финансијска улагања. С обзиром на једносмерну комуникацију ADS–B-а, успостављање поверљиве авионске мреже захтева нови компликован протокол. Такође, требало би узети у обзир и претње од могућих напада ометања, који може деградирати процес мултилатерације.

Фузија података (*Data Fusion*) је техника спајања и корелације података добијених из различитих извора, у циљу добијања тачнијих и поузданијих резултата од оних добијених из једног извора. Идеја фузије података може се извести уз помоћ различитих приступа као што су моделовање засновано на вероватноћи, фази логици и машинском учењу (поглавље 5.3). С аспекта безбедности ADS–B-а, фузија података користи се за проверу података о позицији добијених од ADS–B и других независних извора (нпр. PSR, SSR и MLAT), као и података из плана лета [470, 471]. Свако одступање система од правилног

[188] Процењена удаљеност теоретски означава круг (сферу) са пријемним чвором у центру и предајником на сфери; за прецизно лоцирање мете, потребно је три или више ових сфера.

(нормалног) рада може се сматрати претњом или грешком. Овај приступ омогућава развој аутоматизоване идентификације грешке/претње, као и реакционог система за контролу ваздушног саобраћаја, који испитује корелацију карактеристичних података користећи приступе фузије података (као што је статистичко моделовање или машинско учење) за детекцију недоследности у примљеним подацима и у крајњем исходу, за детекцију напада на ADS–B. Предност фузије података је компатибилност с традиционалним системима навигације, као и то што није потребна модификација ADS–B порука и протокола. Ипак, постоје неки проблеми у вези са фузијом информација добијених различитим техникама, као што је несинхронизација информације о положају преузете од ADS–B система и подацима добијеним из MLAT или GPS-а, а што захтева временску координацију између ових система [472].

Детаљни опис различитих приступа за решавање безбедности ADS–B система, дат је у научним радовима [13] и [460]. Најскорије, предложене су различите технике за ублажавање рањивости ADS–B, као што су оне засноване на моделима машинског учења [473], мрежа дуготрајне меморије (*Long Short–Term Memory*, LSTM) [18], SODA–DNN (*Deep Neural Network*) [19] и MAVPro (*Massage Verification Protocol*) [474].

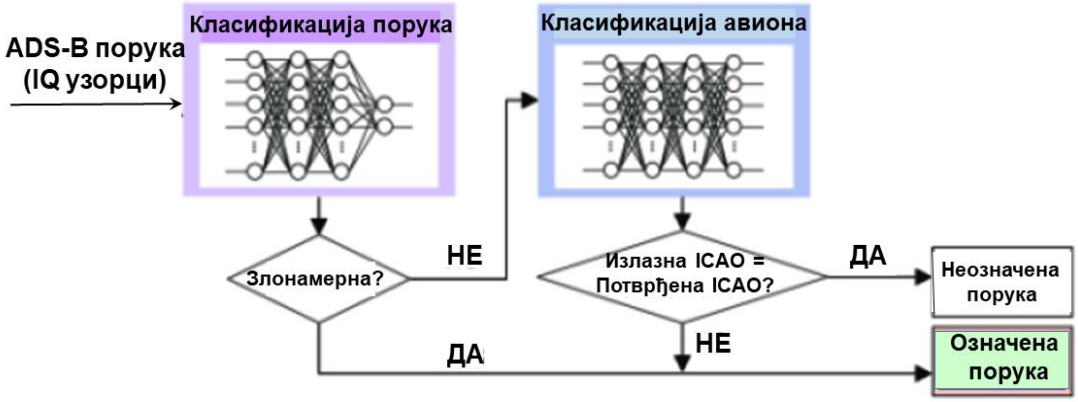
Дакле, за детекцију спуфинга, тј. заштиту бежичне ADS–B комуникације, предложу се различите безбедносне методе/технике, које се заснивају на постојећим криптографским техникама [17, 462, 475]. Алтернатива овим техникама су некриптографски приступи, као нпр. оно који се заснивају на раздвајању сигнала (*PHY-layer signal separation*) [421], верификацији времена и положаја [476], Доплеровом померају [477] и мрежној анализи [18, 19, 449].

Најскорије развијене методе/технике за **детекцију спуфинга** ADS–B система, заснивају се на предикцијама математички постављених модела и мрежној анализи, тј. алгоритмима машинског учења, као што је модел дубоког учења. Једна од ових метода, јесте и метода која се заснива на SODA–DNN (*Deep Neural Network*) спуфинг детектору (сл. 38) [19]. Као што истичу *Xuhang* и аутори, ова техника детектује спуфинг напад с веома великом вероватноћом (99,34%) и незнатним уделом лажних аларма (0,43%), као и идентификује појединачне ваздухоплове с веома великом тачношћу (96,66%), као и средњом F-вредношћу (96,68%), што је значајно унапређење у односу на друге најсавременије детекторе.

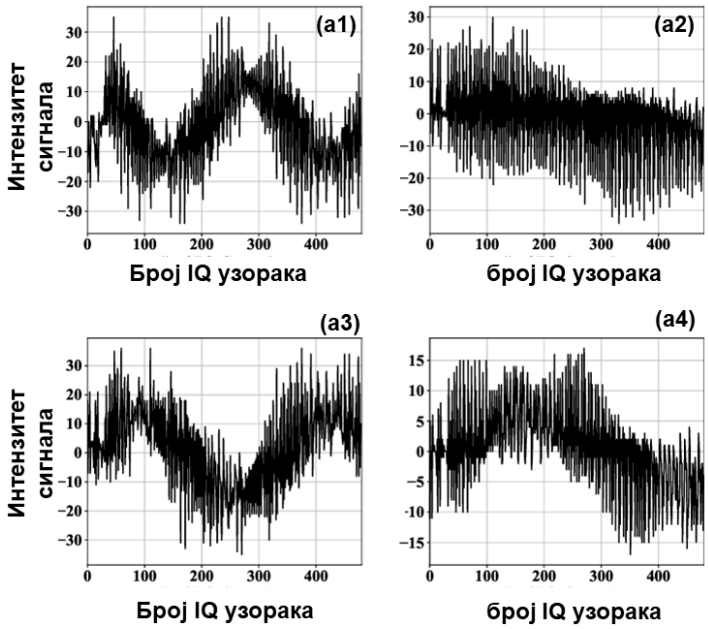
У SODA–DNN техници, за детекцију спуфинга (са земље или ваздуха), користи се SODA–DNN детектор, који се састоји од: класификатора порука и класификатора ваздухоплова.

Тако, SODA–DNN детектор омогућава да станица на Земљи, опремљена ADS–B пријемником, компјутерским ресурсима, адекватном базом примљених аутентичних ADS–B порука сваког авиона, и сл., анализира сваку долазну поруку на основу карактеристика *PHYlayer*-а (IQ узорци и фазе, фуснота 182) и нотира сваку сумњиву поруку. Класификатор порука одређује да ли је ADS–B порука злонамерна или није (сл. 39). Порука која није злонамера, прослеђује се у класификатор ваздухоплова, који, за разлику од класификатора порука (који користи IQ узорке), као улазне податке користи фазе примљених порука;

поређењем ICAO адреса са захтеваном, детектор може открити спуфинг напад (сл. 39а1–а4).

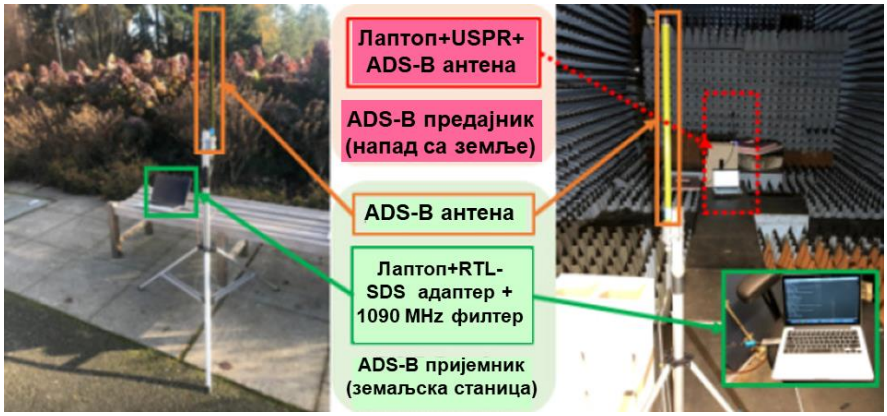


Слика 38. Шематски приказ SODA–DNN методе за детекцију спуфинг напада на ADS–B систем (модификовано и преузето из [19])



Слика 39. Карактеристике различитих порука, аутентична (а1) и малициозних порука (а2–а4) у нападима понављањем поруке (а2), понављањем IQ података (а3) и увођењем ″авиона-духа″ (а4) (модификовано и преузето из [19])

За испитивање карактеристика предложеног детекторског система, неопходно је анализирати велики број реалних података (спуфинг напада), односно располагати адекватном опремом, која обухвата ADS–B ресивер (лаптоп, RTL–SDR адаптер, 1090 MHz филтер и ADS антена) и ADS–B спуфер (лаптоп, SDR и ADS–B антена), који симулира ADS–B спуфинг напад (сл. 40).



Слика 40. Илустрација прикупљања података коришћењем ADS–B пријемника и спуфера базираног на SDR-у. ADS-B пријемник прикупља аутентичне поруке, које преноси SDR спуфер (модификовано и преузето из [19])

Генерално, ефикасност предложене анти-спуфинг технике зависи од нивоа софистицираности уређаја за генерисање спуфинг (лажних) сигнала, тј. сценарија спуфинг напада. Истраживања из ове области имају за циљ налажење осетљиве, брзе, поуздане и робустне методе за детекцију спуфинга. Супериорна анти-спуфинг техника, идеално, требало би да се заснива на једноставним рачунарским алатима, као и да буде ефикасна у случају генеричких сценарија спуфинга, као што су нпр. анти-спуфинг технике које се заснивају на просторној обради сигнала.

Такође, због све веће употребе UAS, и коришћења ADS–B уређаја, као и интеграције UAS у националне системе ваздушног саобраћаја, улога ADS–B постаје све значајнија [478]. Интеграција UAS и ADS–B, представља нарочити изазов, јер се у овом случају може користити електроника слабијег квалитета, а системи не захтевају ригорозно одржавање. Због тога може доћи до ненамерног преноса погрешних ADS–B података, а без механизма за решавање ових проблема, непроверени ADS–B подаци, могли би представљати значајну опасност за авио-саобраћај.

6.3. ЉУДСКИ ФАКТОР У ОДБРАНИ ОД САЈБЕР НАПАДА

Интензивирање коришћења сложених ICT у ваздухопловству, као нпр. авио-системима и системима ATC, креирао је потенцијалне векторе за сајбер нападе, а међузависност између сложених авио-система и њихове интеграције у модерни авион, може једноставно проширити ефекте сајбер напада од једног система до другог. Сајбер-напади на авионе још увек су изузетно ретки, али пратећи тренд веома брзог пораста IT, повећава се и вероватноћа извођења ових напада у будућности, који могу имати катастрофалне последице.

До недавно, истраживачи из области сајбер-безбедности, углавном су занемаривали људски фактор, тј. понашање пилота, који може бити изложен сајбер-нападу. Људски фактор је анализиран у контексту испитивања инжењерских алата, који би задовољили одређене безбедносне захтеве, а анализа људских фактора показала је експлицитну потребу пилота за техничком подршком током сајбер-

напада, као и њихову легитимну бригу у вези с доношењем одлука на основу погрешних/нетачних и на други начин корумпираних информација. Кључни проблем је што успешан сајбер напад, излаже пилоте великој неизвесности, за разлику од суочавања пилота с техничким проблемима (када пилот може применити процедуре за решавање повезаних техничких проблема, добити информације од авио-система о томе како ће специфична техничка неисправност утицати на перформансе авиона, и сл., како би се могли психички припремити).

Када се пилоти суоче са сајбер-нападом, не знају да ли су индикације поуздане или изостају, затим, да ли је проблем решив према процедурама, као што и не знају да ли ће се након примењене процедуре појавити неки други проблем, одмах након имплементиране процедуре. Тако, управљање сајбер-нападима, које вероватно карактеришу двосмислене, тј. нејасне индикације и недоступне опције одговора, веома су напорне за пилота и утичу на његове перформансе.

Приступ проблему сајбер безбедности, у контексту техничког изазова, односи се на интеграцију адекватних техничко-технолошких средстава како би се спречили потенцијални сајбер напади Иако је ово техничка/организациона база, која представља баријеру, и која спречава да сајбер напад продре до авиона/кокпита, неопходно је да посада авиона/пилот, тј. људски оператер буде интегрисан у сајбер-одбрамбени слој, или, шта више, буде последња линија одбране – од одговора летачке посаде/пилота на сајбер напад, зависи да ли ће доћи до потпуног ублажавања или појачавања ефеката сајбер напада.

Због свега тога, веома важан аспект сајбер-одбране, је и узимање у обзир људских фактора, као и проактивни приступ. Најскорије, анализирани су перформансе пилота, који су суочени са сајбер нападом, и то: сајбер-напад на земаљске навигационе системе (MDF VOR земаљска станица) [479], и манипулација система који су потпуно/делимично критични по сигурност [480], а добијени резултати и препоруке ових истраживања биће укратко дати у наставку текста.

Резултати експерименталног истраживања фокусираног на пилоте који су суочени са сајбер нападом [479], показују да исти утиче на све анализиране променљиве (персоналне карактеристике пилота), и то: оптерећење пилота[189] (повећава се), поверење у систем[190] (смањује се), праћење погледа (покрета очију)[191] и перформансе (критеријуми перформанси пилота дефинисани су према томе да ли су исправно решили проблем или не, а процењивани су параметри

[189] Радно оптерећење пилота је квантификовано коришћењем верзије NASA *raw task load index*-а (TLX) [481]. Укупно оптерећење је средња вредност шест подскала (ментална, физичка и временска захтевност, учинак, напор и фрустрација) чије су вредности од 0 (нема оптерећења) до 100 (највеће оптерећење).

[190] Поверење пилота је евалуирано, користећи верзије упитника [482, 483], који је установљен претходно [484]; пилоти су оцењивали своје слагање са 12 тврђења на *Likert*-овој скали од 1 (најслабије) до 7 (најјаче) поверење.

[191] Праћење погледа је квантификовано анализом односа пажње према три дефинисане области од интереса (летење, навигација и управљање системом) и представља однос трајања погледа на специфичну област и укупног трајања погледа на било коју област. Анализа се односила на временски период од 25 s, што је довољно времена да пилот утврди да ли постоји напад или не.

путање лета, с динамиком авиона *Airbus* A320, уз искључен ауто-пилот, тако да је мануелни лет био секундарни задатак, тј. додатно повећање обима посла током решавања проблема. У односу на пилоте, који нису били изложени сајбер нападу, пилоти који су суочени са сајбер нападом, имали су мање оперативне способности, као и укупни учинак. Такође, упозорење о предстојећем сајбер-нападу може ублажити неке од анализираних ефеката, али их не може у потпуности елимисати. Тако, препорука аутора научног рада је укључивање свести о сајбер нападу у периодичну обуку пилота, а будућа истраживања би требало да се фокусирају на развој одговарајућих процедура/техника за обуку пилота, која се односи на детекцију и адекватан одговор на сајбер нападе; осим за пилоте, осмишљавања такве обуке мора узети у обзир целокупно особље на које може утицати потенцијални сајбер-напад.

С обзиром на одговорност коју има [485], и с обзиром на квалитативне резултате до којих су дошли аутори научно-истраживачког рада [479], истиче се проактивни приступ – за минимизирање сајбер напада предлаже се обука пилота за подизање свести о сајбер нападима (врстама претњи, начинима којим се авион може ″заразити″ злонамерним софтвером, и нарочито, свакодневним персоналним активностима које могу ″заразити″ нпр. EFB) али и обука кабинског особља, у циљу успостављања ″колективне свести о сајбер претњама″ [486], као и обука о вештинама општег одлучивања (пилоти би требало да буду обучени за контролисање непредвиђених и неочекиваних догађаја и решавање проблема).

Закључак је и да систем упозорења на сајбер-напад, може бити драгоцено средство подршке за пилоте, али да ови системи упозорења не могу заменити ни пилотско одлучивање, нити обуку пилота у циљу подизања свести о сајбер нападима. Неопходно је истаћи и то да само исправна и поуздана индикација упозорења могу смањити когнитивно оптерећење пилота, као и створити одговарајућу слику ситуације и тако побољшати учинак. С друге стране, нарочиту забринутост изазивају лоше дизајнирани аларми, јер у великој мери, могу повећати стрес/скренути пажњу пилота [487]. Шта више, анализа улоге система за узбуњивање у авио-несрећама, показала је да пилоти често нису успевали да открију или чак разумеју долазна визуелна или звучна упозорења [488].

За разлику од анализе дате у раду [479], која се односи на процену понашања пилота на симулацију сајбер-напада на земаљске навигационе системе (MDF VOR земаљска станица), у раду [480] анализира се аспект људског фактора, при манипулацији система који су потпуно/делимично критични по сигурност[192], и то: *Traffic Collision Avoidance System* (TCAS), *Ground Proximity Warning System* (GPWS) и *Instrument Landing System* (ILS). Показано је да сва три сценарија бежичних

[192] Сигурност (*safety*) се може дефинисати као „степен до којег је случајна штета спречена, откривена и на коју се адекватно реагује“ [489]; у контексту људских ресурса, сигурност је у вези са замором, губитак вештине мануелног летења, сложеном променом задатака, затим, техничким кваровима који захтевају напорно решавање проблема и доношење одлука, као и интензивну тимску комуникацију. С друге стране, безбедност (*security*) се може дефинисати као „степен до којег је злонамерна штета на вредној имовини спречена, откривена и на коју се реагује“ [490]; често се сматра техничким изазовом, али би, при успешном сајбер нападу, реакције пилота вероватно биле сличне онима као код проблема са сигурношћу.

напада, значајно утичу на контролу и изазивају значајне грешке у операцијама прилаза, маневрима избегавања и скретања, додатно проузрокујући оптерећење, неповерење у систем (мету напада); у сваком нападу око 30 % пилота потпуно је искључило авио-систем, чак и у случају када су то били важни сигурносни системи. Пилоти су сматрали да су симулирани сценарији сајбер напада корисни (100 %), као и да би обука на симулатору за бежичне нападе могла бити од значајна (93,3 %). Напад на TCAS идентификован је као најпроблематичнији (комбинује изразиту непријатност и смањење сигурности); напади на GPWS и ILS, такође су представљали проблем, али су их пилоти решавали нешто једноставније. Као што истичу аутори, симулације лета у вези са бежичним нападом или обука, може помоћи и припремити летачку посаду на потенцијални сајбер напад.

Најскорије, још једна значајна област истраживања јесте сајбер-безбедност UAS, с обзиром на огроман пораст употребе дронова у претходној деценији. Тако, у мини-ревијалном раду [491], аутори издвајају следећа кључна питања које би требало анализирати у вези са UAS сајбер-безбедношћу:

- Које су карактеристике оператера рањивих на сајбер-безбедносни аспект UAV и врсте потенцијалних фаталних сценарија?
- Који су начини ефикасног образовања оператера за унапређење својих вештина у вези са UAS сајбер-безбедношћу?
- Који су начини ефикасног избора и рада са запосленима у компанијама које се баве UAS сајбер-безбедношћу?
- На који начин смањити мотивацију нападача?
- Како ће смањење вештина управљања, као последица аутономног управљања, утицати на способност оператера/човека да реагује на проблеме сајбер безбедности?

Аутори закључују да увођење техничко/технолошких побољшања за UAS сајбер-безбедност, не значи нужно и сигурност с аспекта безбедности саобраћаја (аутоматизација која унапређује сајбер безбедност, као нпр. блокирање управљача у опасној ситуацији у циљу онемогућавања промене његовог положаја од стране нападача, није сигурно, јер блокирање управљача, онемогућава оператера да реагује на одговарајући начин). Тако, скреће се пажња на то да се при дизајнирају UAS безбедности, узме у разматрање и безбедност саобраћаја на глобалном нивоу.

За разлику од коришћења традиционалних сајбер тактика, данас нападачи теже стварању суптилне неефикасности која, када се агрегира у читав систем, резултира смањеном ефективношћу система. Циљ оваквих напада је онемогућити њихову детекцију што дуже времена, и тако изазвати велику штету. Оваквим симулираним "ниским и спорим" нападима били су изложени оператери UAS, проузрокујући промену одабране дестинације лета и заустављање UAS [492]. Резултати тестирања показали су да је одређени број учесника (око 64%) приметио манипулацију UAS-ом, али тек након низа питања која су их навела да размисле о проблемима с којима су се суочили током задатка. Добијени резултати у вези са суптилним сајбер нападима дизајнираним тако да постепено деградирају људске перформансе, показују да су ове промене перформанси евидентиране у каснијој фази напада. Без обзира на то, ове промене су ефикаснији показатељ у односу на детекцију оператера.

У ваздухопловству и безбедности, брзи одговор након откривања претње је критичан. Када се деси нешто непредвиђено, на малим висинама лета, а поготово у некој од критичних фаза лета, пилот нема времена да дуго размишља шта треба да уради. Пилоти се уче да ″увек имају излаз″ и да буду спремни да га брзо користе. Технике машинског учења и вештачка интелигенција (*artificial intelligence,* AI) могу се у великој мери користити у домену безбедности као потенцијална решења за ваздухопловну индустрију, као што су детекција аномалија авионике, остваривање безбедности *data link* комуникација, као и безбедносних сертификација [493]. У том контексту, ″док се ваздухопловна индустрија бори против нових претњи усмерених на технологије које су толико критичне за њено пословање, улога вештачке интелигенције у обуздавању ових напада и у борби против њих никада није била важнија″ (*Poppy Gustafsson*, извршни директор *Darktrac*-а[193] [494].

У ваздухопловству, ефикасан одговор се највећим делом ослања на знање и брзе реакције пилота, али у сајбер безбедности, према *Darktrace*-у [494], вештачка интелигенција (*artificial intelligence,* AI) чини одговор бржим и ефикаснијим [495]. *Darktrace Respond* користи *Detect*-ово контекстуално разумевање како би предузео оптималну акцију за ублажавање претње. Прилагодљивост овог одговора је кључна – један сајбер напад може доћи у било ком броју конфигурација, а *Respond* може прилагоди своје акције на одговарајући начин. Дакле, са AI која предузима акције брзином машине, нудећи ефикасне и проактивне мере, као и ″видљивост на чистом небу″, авио компаније/безбедносни тимови могу бити сигурни у своју способност да осујете напад, односно бити/остати заштићене од сајбер напада.

[193] *Darktrace* је глобални лидер у сајбер-безбедносној вештачкој интелигенцији. Базиран је на три технолошка производа: *Detect, Respond* и *Prevent,* засновани на ″само-учећом″ вештачком интелигенцијом, технологијом која не само да гради, већ и континуирано развија своје разумевање посла. Дарктраце-ове одвојене технологије такође уче једна од друге. Свака од три технолошка производа континуирано уноси податке у друге, помажући да се побољшају сопствене способности, као и способности да организације буду заштићене од претњи. То значи да с повећањем броја корисника, средстава или апликација, покривеност организације *Darktrace* такође расте, користећи сваку нову тачку података да побољша своје разумевање и тачност својих акција и детекција.

7. АНАЛИЗА И ПРИКАЗ РЕЗУЛТАТА ИСТРАЖИВАЊА

У овом делу дисертације, дати су еклатантни примери примене ADS–B система, који су анализирани на основу доступних података. У неким случајевима анализа је била лимитирана малим бројем расположивих информација, с обзиром да се иста односила на најскорије примере, а узимајући у обзир да је ADS–B захтевани глобални стандард у комерцијалном ваздухопловству.

Сајбер инциденти, нису само претпоставка, већ су се неки и догодили. Када се узму у обзир они који су познати[194], сматра се да немају опасан/критичан утицај на безбедност авиона и путника. Међутим, узимајући у обзир да, вероватно постоје и сајбер инциденти који нису јавно доступни, сагледавање њиховог утицаја на авио систем, донекле се доводи у питање. Ипак, систематизација и евалуација реалних сајбер инцидената, представљају полазну тачку за предикције будућих трендова сајбер напада, као и развој и имплементације сајбер-противмера у сектору авијације. Примери реалних сајбер претњи/инцидената у цивилној авијацији дати су у делу 7.1.

Застареле технологије у авијацији оставиле су много простора за побољшање безбедности, као и ефикасности летења. При томе, увођење нових технологија, као што је ADS–B у авијацији, праћено је и изазовима, па чак и одређеном врстом скепсе.

Свакако, оно што ADS–B пружа је повећање тачности и прецизности надзора, тако да се катастрофе попут авио-несреће/нестанак малезијског авиона *Boeing* 777 (MH370), описане у делу 7.2.1, могу избећи коришћењем интелигентне ADS–B технологије. С друге стране, концепт аутономног летења за *e-Enabled* авионе, као нпр. авиона компаније *Boeing* или *Airbus*, доводи до пораста сајбер рањивости авиона. У вези са тим, у делу 7.2.2., описана је фатална несрећа авиона *Boeing* 737 MAX 8, након које су сви *Boing*-ови авиони овог типа приземљени.

Осим бројних бенефита (описаних у делу 6.1.4), тачност и широк спектар ADS–B података који се могу складиштити, омогућава проактивно решавање различитих екцесних/конфликтних или хитних ситуација у авијацији, јер се подаци с одређеног лета ажурирају на остале (и авионе које су актери инцидентне ситуације, као и све друге, који нпр. учествују у проналажењу/спашавању). Све већа доступност телеметријских ADS–B података, од велике су користи експертима, научницима и истражитељима авио-инцидената/несрећа, који методично и систематски разматрају доказе и анализирају све потенцијалне факторе како би утврдили потенцијални узрок инцидента. Управо одређени ADS–B подаци указују на детаље инцидентних ситуација у ваздухопловству. У вези са тим, одабрани/евидентирани примери описани су у поглављу 7.3.

Дизајн истраживања који се користи у овој дисертације је квалитативна и интерпретативна анализа за сагледавање и унапређење дискусије у вези са

[194] Чињеница је да су доступни извори у вези са пријављеним/реалним сајбер инцидентима у сектору цивилног ваздухопловства, ограничени; као пто истичу *Ukwandu*-а и аутори [496], доступан је веома мали број публикација, тј. рецензираних радова у научним часописима и зборницима радова конференција, а с обзиром на период за претраживање објављених научних радова (20 година).

имплементацијом ADS–B и проактивним научним приступом у разумевању потребе за увођењем нових технологија у сектор авијације, као и изазова које ове иновације доносе, нарочито из угла пилота. Истраживање је засновано на научним публикацијама/радовима, званичним ваздухопловним документима, извештајима базираним на *web*-у, новинским чланцима и извештајима о прописима и сличним информацијама регулаторних агенција.

С обзиром на тематику, као и тежњу за актуелношћу, анализа неких од евидентираних примера не садржи коначне закључке, али, осим што су информативне, овакве анализе истичу и улогу људског фактора, као и очекивање да ће пилоти у стресним ситуацијама боље реаговати уколико познају рад система, као и имају сазнање да ADS–B систем обезбеђује поуздане и правовремене податке.

7.1. ПРИМЕРИ РЕАЛНИХ САЈБЕР ИНЦИДЕНАТА/ПРЕТЊИ У ЦИВИЛНОЈ АВИЈАЦИЈИ

Преглед сајбер претњи/напада у сектору цивилног ваздухопловства омогућава идентификовање најчешћих актера претњи, њихове мотивације, врсте напада и мапирање рањивости у ваздухопловној инфраструктури, а које су најчешће подложне сајбер нападима.

У том контексту, у Табели 10 дати су документовани сајбер инциденти/напади у области цивилног ваздухопловства, на основу мапирања сајбер претњи/инцидената датих у ревијалном раду *Ukwandu Ben-Farah* и аутора (период 2001–2022) [496] и мастер раду *Camilo Andres Pantoja Viveros*-а (период 1997–2014) [497], којима су додати они до којих је дошао аутор претраживањем доступних литературних извора током писања мастер рада [3], као и ове докторске дисертације.

Табела 10. Преглед сајбер безбедносних инцидената у авијацији (1997–2023)

Година	Опис инцидента
1997	Упад хакера у *Bell Atlantic* рачунарски систем, што је довело до гашења светла на контролном торњу, као и писти [498]
2003	Један од FAA административних сервера компромитован је нападом *slammer* црва, због чега су интернет услуге у неким деловима Азије биле онемогућене, а што је успорило интернет везе широм света [499]
2006	Убачени вирус у системе контроле ваздушног саобраћаја FAA изазвао је прекид рада дела система ATC на Аљасци [498]
2007	Вирус унет у *Thai Airways Electronic Flight Bags* онеспособио је овај систем и проширио се на друге уређаје истог типа (таблети и ајпеди) [498]
2008	• 800 детектованих сајбер инцидентних упозорења у објектима ATC, од којих преко 150 инцидената још увек није решено [498]

2008	• Хакери су преузели и украли административну лозинку међусобно повезаних мрежа FAA у Оклахоми. Добијањем приступа домену региона западног Пацифика, приступили су на више од 40.000 акредитива за пријаву (користе се за контролу дела FAA мреже за подршку) [500]
2009	• Возач камиона, који који је поседовао ометач GPS-а, ненамерно је изазвао застој у раду *Newark Liberty International Airport's ground-based augmentation system* [342] • Напад на FAA рачунаре, који је омогућио хакерима приступ личним фајловима садашњих и бивших запослених (око 48.000) у FAA [498]
2011	Група софтверских инжењера оптужена је за саботажу у програмском коду, што је довело до прекида рада *check-in* сервиса и отказивања великог броја летова на многим аеродромима [501]
2013	• Гашење система пасошке контроле на полазним терминалима Истанбул *Ataturk* и *Sabiha Gokcen* аеродромима, због напада малвера, што је довело до одлагања бројних летова [502] • Злонамерни напади хаковања и *phishing*-а циљани на око 75 аеродрома у USA, које је према тврђењима извршила неоткривена држава, која је покушала да пробије мрежу америчке комерцијалне авијације [503]
2014	Нестанак бројних авиона са радара у Аустрији, Немачкој, Чешкој и Словачкој; узрок томе, наводно, биле су војне вежбе [504]
2015	DDoS напади на рачунаре за планирање летова на варшавском аеродрому, због чега авионима нису могли бити прослеђени планови лета; ови напади изазвали су отказивање и кашњење на десетине летова [505]
2016	• Авионски системи у USA, Турској, Шпанији, Шведској и Пољској били су заражени малвером, што је довело до кашњења, губитка информација и растуће забринутости запослених у јавном сектору, индустрији и регулаторним телима [506] • Оштећење *website* вијетнамских авио-компанија у Хо Ши Мину и Ханоју, као и аеродромских екрана за информације о летовима, на којима су биле приказане поруке које подржавају кинеске поморске претензије у Јужном кинеском мору од стране пропекиншких хакера [507] • Напад малвера на рачунар IT мреже главног аеродрома у Кијеву, као и ATC [508]
2017	• Међународни аеродром у Одеси био је мета сајбер напада, а малициозни софтвер је паралисао рачунаре на овом украјинском аеродрому [509] • Квар компјутерског система британског националног превозника, изазван искључењем и поновним повезивањем напајања *data-center*, од стране инжењера по уговору. Непријатност због овог инцидента имало је око 75.000 путника *British Airways*-а [507]

2018	• Хакери су украли личне и финансијске податке од око 380.000 путника, који су резервисали авио карте преко вебсајта ba.com и апликације *British Airways app* [510] • Повреда података (око 9,4 милиона) личних података клијената *Cathay Pacific Airways* (Хонг Конг) [511] • Продавнице *Delta Air Lines Inc*. и *Sears Departmental* (USA) пријавиле су повреду података (око 100.000 информација о плаћању купаца) од стране треће стране [512] • Напад на електронске екране, који приказују информације о летовима на аеродрому у Бристолу, што је довело до искључења екрана, који су замењени белим таблама; штетни ефекат овог напада, није познат [513] • *Air Canada* је пријавила повреду података мобилне апликације, што је омогућило да неовлашћена особа има увид у личне податке око 20.000 људи [514] • Повреда података на серверу NASA, што је довело до могућег компромитовања личних података запослених 23. октобра 2018 [515]. • Напад компјутерским вирусом *WannaCry* на *Boeing* (Чикаго); према извештајима компаније, напад је изазвао минималну штету на интерним системима компаније [516]. • Сајбер-напад покренут од стране руске APT групе (АПТ28), који је блокирао АТС Шведске, приземљивши стотине летова у периоду од 5 дана [139].
2019	• Отказано преко 400 летова у USA због проблема у вези са ADS–B системом [517] • Израелске аеродромске власти блокирале су око 3 милиона ботова у једном дану, док су покушали да провале у аеродромске системе [518] • Сајбер инцидент као резултат неовлашћеног приступа *Commercial Aircraft business* (*Airbus*) информационим системима (*Toulouse, France*); према извештајима о комерцијалним операцијама није било утицаја на компанију *Airbus* [519] • *Ransomware* напад на *Albany International Airport* (USA), у коме су нападачи успешно енкриптовали целокупну базу података аеродрома, захтевајући од власти да плате откуп за декрипциони кључ [520] • Истраживачи *Cyberbit*-а, открили су преко свог сигурносног софтвера (EDR), малвере за рударење криптовалута, на више од 50% *workstations* европских аеродрома [521] • *Phishing* напад усмерен на клијенте *Air New Zealand Airpoints*; напад је компромитовао личне податке око 112.000 клијената, с именима, детаљима и *Airpoints* бројевима [522]
2020	• Сајбер инцидент (Денвер, USA) у коме је нападач приступио и украо податке компаније, који су касније доспели на мрежу [523]. • Наводно хаковање једног од система индијске авио-компаније *SpiceJet* – амерички истраживач из области сајбер-безбедности је користећи

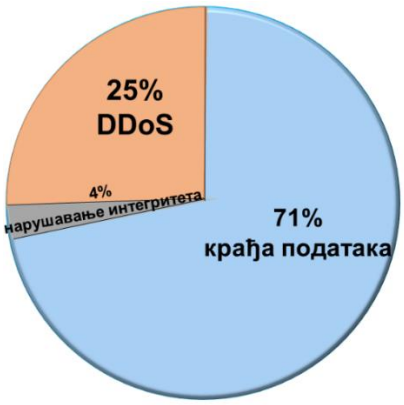
2020	једноставну лозинку приступио нешифрованој резервној копији базе података, с приватним информацијама више од 1,2 милиона путника [524] • Повреда података свемирске подстанице *ST Engineering*, USA, што је касније довело до *ransomware* напада од стране *Maze Cyber-criminal* [525] • Напада *ransomware*-а на произвођача авиона *Embraer*. Као освета хакера за одбијање компаније да плати откупнину, компромитовани подаци појавили су се на новом "црном" веб сајту креираном за објављивање преузетих информација [526] • Компанија која обезбеђује делове великим ваздухопловним компанијама, као што је *Boeing*, била је мета напада новог типа *ransomware*-а који може и да шифрује датотеке и ексфилтрира податке [527] • Истраживачи су показали да се може лажирати TCAS-а, користећи *Digital Video Broadcasting* USB преносиви модем и лажни транспондер, за комуникацију с авионом. Пажљиво постављање "лажних" авиона, може активирати TCAS и упозорити пилота, тј. аутопилота (нпр. у *Airbus*-овим авионима) да се попне/спусти како би избегао судар. Упозорења за извођење ове врсте сајбер напада су различита (нпр. уколико је TCAS *Resolution Advisory* систем искључен, не може доћи до хаковања, а уколико дође до хаковања, лажни авиони се неће појавити на радару, тако да пилот може занемарити упозорења и сл.) [528]
2021	• Софтверска грешка у IT систему, због које није уочено неслагање масе авиона према утоварном листу и плану лета, због чега је авион имао 1606 kg већу масу при полетању него што је захтевано [529] • Напад *ransomware* (LockBit) на *Bangkok Airways* што је резултирало увидом у више од 100 GB података, јер је авиокомпанија одлучила да не плати откупнину; подаци су се углавном односили на пословне документе, али и личне податаке путника (имена, националност, пол, број телефона, е-пошту, адресу, податке о пасошу, историју путовања, бројеве кредитних картица и сл). Према изјавама Тајландског регионалног авиопревозника, ниједан оперативни/ваздушни безбедносни систем није био угрожен овим нападом [530] • У сајбер нападу на авиокомпанију *Air India,* компромитовани су подаци милиона клијената [531]
2022	• *Ransomware* напади на индијску авио-компанију *SpiceJet,* који су, према тврдњама авиокомпаније, брзо отклоњени [532] • Сајбер напад на *Jeppesen* (*Boeing*-ову филијалу), који је утицао на одређене производе и услуге планирања лета, а према изјавама званичника *Boeing*-а, овај инцидент није представљао претњу по безбедност авиона или летења [533] • Истраживачи са Универзитета Мичиген и NASA открили су значајне рањивости у мрежној технологији (мрежни протоколи и хардверски систем, тј. временски активираним етернет) која се широко користи у

	критичним инфраструктурама као што су свемирске летелице, авиони, системи за производњу енергије и индустријски контролни системи [534]
2022	• Непознати хакери, у координисаном нападу, привремено су онеспособили јавне *web*-сајтове најмање неколико великих америчких аеродрома. Није издатио саопштење ко стоји иза ових напада [535] • Откривено да је злогласна (најактивнија) севернокорејска хакерска група „*Lazarus*“ инсталирала *rootkit* за злоупотребу *Dell* хардверског драјвера, чије су мете *spear-phishing*-а током 2021. године, били ваздухопловни стручњаци у Холандији и белгијски политички новинар [536] • Талас шпијунски активности иза којих стоји група нападача, који су раније били повезани са Spy RAT (*spreading remote access trojan*) усвојила је нови алат за покретање напада на низ владиних и државних организација у бројним азијским државама [537] • Напад малвера изазвао је прекид и нефункционалност сателитског широкопојасног приступа *Viasat*-у у Европи, који се повезује са руским деструктивним VPN филтером, и почетком рата у Украјини [538] • Снажан и ефикасан сајбер напад на инфраструктуру Руске Федералне агенције за ваздушни саобраћај (Росавиатсиа) у коме су избрисана сва документа, фајлови, и сл. (око 65 терабајта података) [539]
2023	• Откривање базе података, тј. копија ″листе забрањених летова″ америчке TSA, услед погрешног конфигурисања складиштења података у *cloud*- у. Иза сајбер напада стоји швајцарски хакер (познат као ″*maia arson crimew*″), који је податке пронашао на серверу [540] • Откривање личних података клијената програма лојалности авиокомпанија *Air France* и KLM [541]

Анализом сајбер напада, закључује/доказује се да главне претње у сектору цивилне авијације у вези су с *Advance Persistent Threat* (APT) групама (фуснота 93), које делују, у сарадњи са одређеним државним актерима, у циљу крађе интелектуалне својине и поверљивих података како би унапредили своје ваздухопловне способности, као и надгледали, инфилтрирали и вршили субверзивне активности. Како су полазали *Ukwandu* и аут. [496], најчешће се напада IT инфраструктура – најчешћи тип напад је злонамерно хаковање у циљу добијања неовлашћеног приступа (71%), а затим следе напади усрећивања услуга, који угрожавају доступност података, тј. DDoS (25%) и напади чији је циљ оштећење интегритета датотека (4%) (сл. 41). Према географској одредници, већина сајбер напада забележен је у Северној Америци (од тога око 40% у USA, а само 4% у Канади)[195], затим следе Европа (највише у UK) и Азија, а за Африку, нема расположивих података. Свакако, најбројнији сајбер инциденти икада (око 5 дана непрекидног приземљења авиона), догодили су се 2018. године, а најзабрињавајући,

[195] Удео сајбер инцидената мора се посматрати релативно, тј. у односу на укупан број аеродрома у датој држави/регији/континенту и сл.

догодио се 2019. године, када је више од 50% европских аеродромских рачунских центара, било заражено малициозним софтвером за рударење криптовалута [542], а што је детектовано *Cyberbit*-овим софтвером *Endpoint Detection and Response* (EDR).



Слика 41. Удео различитих врста сајбер напада на IT инфраструктуру сектора цивилне авијације (модификовано и преузето из [496])

У табели 11, дате су неке од потенцијалних рањивости, уочене од стране ваздухопловних организација, хакерске заједнице и медија.

Табела 11. Преглед потенцијалних сајбер рањивости у авијацији (2008–2016) [153, 501, 543, 544–547]

Година	Опис
2008	Дизајн и инфраструктура *Boeing*-а 787, према наводима FAA, омогућава нове врсте конекције путника с подацима на мрежи, које су раније биле изоловане, а сада су конектоване са системима за обављање операција кључних за безбедност лета [543]
2010	Према FAA, неки компјутерски системи *Boeing*-а 747-8 і 747-8F, могу бити рањиви на екстерне сајбер нападима, услед карактеристика њихове конекције [544]
2012	• *Andrei Costin* предочио је слабости у систему ATC; употребом јефтине технологије, уређаја и софтвера, могуће је имитирати ADS-B сигнале и тако убацити "авион-дух" на дисплеј ATC [501] • Потенцијална рањивост у програмирању EFBs, који могу бити корумпирани током ажурирања, при конекцији уређаја с екстерним мрежама [501]

2013	Хакер је демонстрирао да је теоријски могуће, коришћењем *Android* телефона, извршити напад/отмицу на даљину [153]
2014	Експерт за безбедност је саопштио да је наводним успешним хаковањем авиона (преко *Entertainment* система за забаву путника), управљао авионом током лета [545]
2015	Авион *WestJet*-а је наводно емитовао кôд 7500, који указује на отмицу; постоји могућност да је та модификација била изазвана сајбер средствима [546]
2016	Стручњаци за сајбер безбедност, који су радили у сарадњи са DHS-ом, хаковали су *Boeing* 757 на међународном аеродрому у *Atlantik City* (*New Jersey*) преко радио комуникације [547]

У циљу сагледавања утицаја које сајбер претње имају на авијацију, као и њихове распрострањености, у наставку текста дате су неке од круцијалних јавно доступних претњи на авио систем. При томе, аспект одговорног откривања постојећих рањивости, веома је важан, нарочито из угла њихове експлоатације.

- **Контрола летења.** На самиту о безбедности (Амстердам, 2013) [153] *Hugo Teso*, професионални пилот и стручњак за сајбер безбедност, као што је поменуто, показао је да је могуће преузети контролу система за летење и комуникацију, коришћењем *Android Smartphone*. Развијени специјални кôд за "упад" (назван *SIMON*) и андроид апликација *PlaneSploit*, омогућили су потпуну контролу система за летење, као и пилотовог дисплеја у симулираним условима. Тако, хакер може променити смер и брзину летења користећи *handset*, и извршти потпуну модификацију навигације авиона. Такође, показано је да ADS–B није потпуно безбедан и да комуникација авиона може бити пасивно прислушкивана/активно прекинута. Иако према наводима FAA, овакав хакерски напад није могућ на сертификованом авиону, скренута је пажња на неке од пропуста у обезбеђивању сајбер безбедности авиона.

- **Авион**. Према наводима FAA (2008), конекција путничке кабине *Boeing-а 787 Dreamliner* с контролним, навигационим и комуникационим системима, тј. на тај начин контролисани систем авиона, рањив је на сајбер нападе. Компанији *Boeing* је саветовано да реши овај проблем. Поменута конекција изазвала је забринутост, делом и због нових апликација на телефонима (нпр. *Gogo Text&Talk*), које омогућавају путницима да примају и шаљу поруке преко Wi-Fi мреже док је авион у ваздуху. Овај сервис представља безбедносну претњу, с обзиром на то да нема могућност шифровања порука и није сигуран/безбедан (као ни било која друга јавна мрежа).

Илуистрација велике опасности постојања рањивости рачунара, који је повезан на мрежу, тј. од *malware*-а (део 2.1.2 и 3.1.1), јесте фатална **несрећа авиона** *Spanair*-а (лет 5022), одмах након полетања (2008). Детаљније о анализи несреће овог авиона погледати у [548]. Истрага шпанске државне комисије за акциденте и инциденте у цивилној авијацији, показала је да је до ове авио несреће, у којој је

погинуло 154 особе, дошло због тога што је централни компјутерски систем, који се користи за мониторинг техничке исправности/проблема авиона био заражен *trojan horse* рачунарским вирусом. Наиме, рачунар је требало да алармира, тј. покаже на монитору алармни сигнал, као упозорење пилотима, на постојање три техничка проблема пре полетања авиона, што је изостало. Пилоти су покушали да полете, у неправилној конфигурацији, и то, с потпуно увученим флапсовима и слотовима, при чему се није огласило звучно упозорење у кокпиту. Одсуство аларма било је узроковано кваром на системима за активирање система за упозорење. При свему овоме, *malware* је могао продрети у систем на различите начине, као нпр. преко уређаја трећих лица, или преко даљинске VPN конекције (фуснота 59). Овакав инцидент би се могао поновити, и сматра се и да ће се највероватније и поновити.

Такође, тежња авиокомпанија да омогуће својим путницима комфорније путовање (нпр. *Lufthansa* у својим авионима типа *Airbus* A350–900, омогућава путницима да користе погодности *FlyNet* технологије и унапређеном сурфовању; већи екрани омогућавају напреднији кориснички приступ), уводе нове безбедносне ризике, због чега ове везе морају изоловане од конекција које се користе за авио-операције [4].

- **Авио-компаније** –*website* и мреже. Као што је претходно поменуто, за нападе на авио-компаније, користе се различити алати, односно вресте напада, као што је поменути *Sykipot,* који инфицира мету употребом *spear-phishing* tehnika[196] или DDoS напада (део 2.1.2). На пример, израелска национална компанија *El-Al*, била је главна мета за политички инспирисан сајбер напад (2012), у коме је *website* ове компаније био привремено угашен од стране хакера организације *Nightmare Group,* иако интерни системи и распоред летења нису били угрожени. Затим, група *Qods Freedom* је тврдила да је хаковала (2013), поред других израелских вебсајтова и вебсајт *El-Al* компаније, и преузела сајт у планираном DDoS нападу.

- **Аеродроми и пограничне власти**. Еклатантни пример сајбер инцидената на аеродромима, је екцес, који се догодио 5. септембра 2013. године, због кога су улази и излази од, и до, међународне турске границе били затворени. Узрок су били проблеми у *Police Intra-net* систему (PolNet). Иако је турска *RedHack* хакерска група преузела одговорност за овај сајбер напад, полиција је демантовала тврдње хакера, наводећи да је сајт био затворен "контролисаном" деактивацијом због трансфера података. И раније је било напада на PolNet систем (два пута у децембру 2012. године), али нико није преузео одговорност за напад; резултат тих напада био је прекид рада система пасошке контроле, тј. привремени прекид рада базе података PolNet система на *Atatürk* и *Sabiha Gökçen* међународним аеродромима, а према наводима *Hurriyet Daily News*, разлог пада мреже био је сајбер напад изазван непознатим рачунарским вирусом. Такође, хакерске групе *Hackers of Portugal Cyber Army* и *HighTech Brazil HackTeam* (април, 2013. године) објавили су да су "пробили" официјални сајт *Dubai International Airport*-а, који је хостован на домену

[196] *Spear-phishing* је e-mail или електронска комуникациона превара усмерена на појединца/организацију, у циљу крађе података/инсталирања *malware* на рачунар корисника.

dubaiairport.com, доводећи до онлајн "цурења" *e-mail* адреса и лозинки особља. Мотивација хакера је нејасна.

У табели 12, дати су неки сајбер безбедносни инциденти, као илустрација њиховог различитог утицаја на аеродромске операције [2, 3, 202]

Табела 12. Преглед сајбер безбедносних инцидената на аеродромима (2016–2023) [202]

Година/Држава	Опис
2016/ USA	Путници широм света су се нашли у незавидној ситуацији, након што је нестанак струје приморао америчку авио-компанију *Delta* да суспендује летове. Целовечерњи нестанак струје у Атланти, у близини авио-компаније, довео је до деградације рачунарских система, и тако до отказивања *check-in* система, екрана за обавештавање путника, *website* авио-компаније, као и *smartphone* апликација
2016/ Вијетнам	Успешни сајбер напади на два највећа аеродрома и највећу националну авио-компанију у Вијетнаму (*Vietnam Airlines*) у којима су хакери, накратко, преузели екране за информисање путника, као и системе за озвучење. Екрани, као и озвучења емитовали су анти-вијетнамске и анти-филипинске поруке, због чега су аеродромске власти угасиле оба аеродромска система. У исто време, *website* авио компаније је био такође хакован и пребачен на малициозни инострани сајт, док су подаци путника били злоупотребљени. Због свега овога, вијетнамске власти спровеле су свеобухватну проверу уређаја и технологија произведених у Кини, а које се користе на вијетнамским аеродромима, јер се претпостављало да кинеска хакерска група 1937cn, може бити одговорна за нападе
2016/Италија	Покушај потпуног онеспособљавања аутоматизованог *check-in* система на римском аеродрому *Fiumicino*, што је резултирало двочасовним застојем оперативности овог система. Напад је био неуспешан захваљујући интернет провајдеру који пружа услуге аутоматизованом *check-in* систему за приступ и обраду података путника
2016/UK	Након слетања, пилот *British Airways*-а (лет из Женеве) пријавио је колизију с дроном приликом приближавања лондонском аеродрому *Heathrow*. Овај инцидент је актуелизовао разматрање проблема дронова, тј. штете које могу проузроковати авионима с посадом
2016/Широм света	Произвођач цивилних ваздухоплова *Airbus Group* је жртва око 12 сајбер напада годишње, и то углавном у циљу изнуде и других акција, које извршавају хакерске групе, и то веома често, уз подршку различитих држава

2017/UK	Аеродромима у UK издата су упозорења да појачају одбрану због забринутости да ће терористи, првенствено Ирака и Леванта (Исил), користити технике да заобиђу уређаје за проверу на европским и америчким аеродромима, због чега је у UK и USA забрањено путницима из многих држава да уносе лаптопове и друге електронске уређаје у авион [549]
2017/Аустралија	Сајбер напад на компјутерски систем аеродрома у Перту од стране хакера из Вијетнама, који је украо осетљиве безбедносне податке и грађевинске планове аеродрома, користећи акредитиве "треће стране" за приступ компјутерским системима аеродрома [550]
2022/UK	Отказани летови *British Airways*-а са аеродрома *Heathrow* услед, према саопштењу авиокомпаније, "техничких проблема", tj. хардверских проблема, а не сајбер напада [551]
2022/Швајцарска	Напад *ransomware* на швајцарску служба за управљање аеродромима (*Swissport*), који је био усмерен на њену IT инфраструктуру. Није именована група која стоји иза овог сајбер напада [552]
2023/Немачка	Отказивање бројних летова, немачке авио-компаније *Lufthansa* услед проблема с компјутерским системима за пријаву и укрцавање путника на аеродрому у Франкфурту, због чега је приземљено на стотине авиона ове компаније; према саопштењу компаније, софтверски проблеми су узроковани оштећењем широкопојасних каблова *Deutsche Telekom*-а [553]

Генерално, преглед пријављених/познатих сајбер инцидената, затим, анализа опсега површина напада, као и постојеће динамике претњи, веома су значајни и представљају полазну тачку за предвиђање будућих трендова сајбер напада. Закључци до којих се долази оваквим анализама, могу бити/су подршка будућег дефинисања и имплементације проактивних мера, које штите сектор цивилне авијације од сајбер инцидената, а који нарушавају поверење корисника у овој кључној индустрији оријентисаној на услуге.

7.2. ПРИМЕНА ADS–B ТЕХНОЛОГИЈЕ: СТУДИЈЕ СЛУЧАЈА

ADS–B технологија је недвосмислено решење за многа питања у вези са одрживошћу ваздухопловне индустрије – с повећањем прецизности информација, ADS–B омогућава генерисање краћих оптимизованих путања лета авиона, резултирајући скраћењем времена лета, као и смањењем трошкова и емисије штетних гасова. Штавише, с овом напредном технологијом, сигурност лета је подигнута на виши ниво. Нажалост, за трагичну авио-несрећу/нестанак малезијског авиона *Boeing* 777 (MH370), која је описана у делу 7.2.1, између осталог, ADS–B није био обавезни глобални стандард, а постао је то тек касније. С друге стране, достигнућа еволуције информационих технологија имплементирани су на свим

нивоима авијације – од побољшања система за надзор, навигацију и комуникацију до апликација које пилоти користе за примање, складиштење и приказивање релевантних ваздухопловних информација, што се користи за доношење одлука у кокпиту. Највећи изазови модернизације, односе се на рањивости авио-софтверских система на сајбер нападе, а што може, у крајњој истанци, довести до лоше процене пилота. Тако, погрешни/неизвесни подаци и фактор стреса, повезани с континуираним погрешним порукама и критично време за захтевани одговор пилота, повећава и утиче на сигнурност и безбедност лета. У вези са тим, пример фаталне несреће етијопијског *Boeing*-а 737–800 Max описан је у делу 7.2.2.

7.2.1. Фатална несрећа/нестанак малезијског авиона *Boeing* 777 (MH370)

Нестанак авиона *Boeing* 777 (MH370), тзв. нестанак MH370 **(**8. март 2014), на лету од Куала Лумпура (Малезија) ка Пекингу (Кина), са **227 путника и 12 чланова посаде**, довео је до највеће потраге у историји ваздухопловства, која је обухватила област од Индијског океана (западно од Аустралије) до централне Азије. Ово је и једна од највећих мистерија у модерној авијацији, с обзиром на непознати узрок нестанка, тј. његову збуњујућу природу [553] – авион (сл. 42) никада није стигао до Кине, већ је нестао негде изнад Индијског океана. Нестанак авиона, покренуо је вишегодишњу потрагу (копном и морем), која је на крају обустављена без икаквих закључака, али је коштала милионе долара [554].

Слика 42. Малезијски авион *Boeing* 777 (MH370) који је мистериозно нестао 8. марта 2014. (слика модификована и преузета из [555])

Чињенице и коментари

На основу објављених података, чињенице у вези са нестанком авиона *Boeing* 777 (MH370), 8. марта 2014. године, су следеће [555, 556]:

00:41 (16:41 GMT, 7. март) – авион *Boeing* 777 (MH370) полетео је с међународног аеродрома у Куала Лумпуру (Малезија) и требало је да стигне у Пекинг (Кина) у 06:30 (22:30 GMT[197]).

[197] GMT (*Greenwich Mean Time*) – средње време по Гриничу.

Авион је достигао висину крстарења од 35.000 ft (10.700 m) у 01.01. Према саопштењу *Malaysia Airlines*-а, авион је изгубио контакт за мање од сат времена након полетања. При томе, авион није послао никакав захтев за помоћ или поруку.

01:07 Авион је послао своју последњу ACARS поруку (ACARS систем се користи за слање дигиталних порука у оба смера, авионима, авио компанијама и другим ентитетима авио система, део 3.1.2.1); следећа, очекивана ACARS комуникације требало је да буде у **01:37**, међутим, до тога није дошло, тј. авион није послао очекивану поруку.

01:19 Последња комуникација између авиона и малезијске АТС.

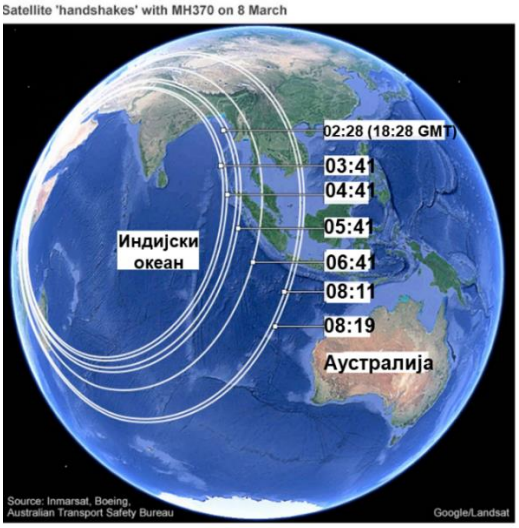
Авио-компанија је саопштила да су према првим истрагама, последње речи пилота биле "У реду, лаку ноћ". Међутим, малезијске власти су касније саопштиле да су последње гласовне радио-трансмисије из авиона, биле речи „Лаку ноћ, малезијски три седам нула“, које је изговорио пилот авиона MH370.

01:19 – (**~01:21)** Искључен транспондер авиона, који комуницира с земаљским радаром, тј. АТС, када је авион прешао из малезијске АТС у ваздушни простор Вијетнама изнад Јужног кинеског мора.

01:21 Управа за цивилно ваздухопловство Вијетнама саопштава да се авион није пријавио према плану контроле летења у Хо Ши Мину.

02:15 Малезијски војни радар детектовао је лет MX370 на тачки јужно од острва Пукет у Малачком мореузу, западно од његове последње познате локације. Такође, тајландски војни радарски дневници, потврдили су да је авион скренуо на запад, а затим на север преко Андаманског мора. На мапама које прате извештај од 1. маја 2014. год., Влада Малезије је ревидирала време на **02:22** и поставила координате лета авиона западније.

02:28 (18:28 GMT, 7. март): Након губитка авиона са радара, сателит изнад Индијског океана добио је податке из авиона, у облику седам аутоматских размена порука, према принципу „руковања“ (*handshakes*) између авиона и земаљске станице Први *handshakes* је био у 02:28 по локалном времену (сл. 43).



Слика 43. *Handshakes* трансмисије које је забележио сателит (08. 03. 2014. год.) (слика преузета из [555])

08:11 (00:11 GMT, 8. март) Последњи потпуни *handshakes*.

Ове информације (објављене недељу дана након нестанка авиона), сугеришу да је авион могао бити у једној од две путање, првој, која се простире северно, између Тајланда и Казахстана, или другој, која се протеже на југ између Индонезије и јужног Индијског океана. Наиме, сателит *Inmarsat* у гео-стационарној орбити изнад Индијског океана, који је примао сигнале с лета MH370, последњи пут је детектовао авион у 08.11.

08:19 Међутим, постоје докази о даљем "делимичном *handshakes*-у" између авиона и земаљске станице, и односио се на упит авиону за пријаву.

Према истражитељима, овај *handshakes* је у складу са ситуацијом оспособљавања сателитске комуникационе опреме у авиону након нестанка, као нпр. прекида напајања електричном енергијом.

09:15 Требало је да буде следећи заказани аутоматски контакт између земаљске станице и авиона. Међутим, одговора из авиона није било.

Потрага

Нестанак авиона *Boeing* 777 (MH370) довео је до мултинационалне потраге, у којој су учествовале Владе Малезије, Кине и Аустралије. У овој потрази, коришћени су комуникациони дневници, као и подаци војног и цивилног радара. Међутим потрага за авионом била је безуспешна, наводећи истражитеље и авио-експерте на спекулације да до овог нестанка авиона не би дошло да је била раније развијена ADS–B технологија [554].

Потрага за несталим авионом MH370 обустављена је 2017. године, након скоро три године дугог претраживања морског дна Индијског окена (површине 46.000 km^2), тако чинећи ову авионску трагедију једном од највећих мистерија у авијацији свих времена. Ова најсложенија и најскупља потрага у историји ваздухопловства (коштала је око 150 милиона долара) [557], завршена је без коначних резултата – поред тога што није успела да лоцира авион, није одговорила ни на питање узрока његовог нестанка. Авион који је превозио 239 људи из Куала Лумпура, главног града Малезије, до Пекинга нестао је са цивилног радара у раним јутарњим сатима 8. марта 2014, без икаквог позива у помоћ од стране пилота. Како је наведено (2017) у саопштењу аустралијског *Joint Agency Coordination Center* [558], "Упркос свим напорима користећи најбољу доступну науку, најсавременију технологију, као и моделирање и савете високо-квалификованих професионалаца који су најбољи у својој области, нажалост, потрага није успела да лоцира авион". Управо у овој изјави најбоље се препознаје права вредност нове ADS–B технологије и њених ванредних могућности, као и остварење дугогодишњег циља ваздухопловне индустрије за глобалним праћењем авиона у реалном времену.

Почетна потрага за авионом била је фокусирана на Јужно кинеско море (јужно од вијетнамског полуострва Ка Мау), с обзиром на то да би према планираној рути, авион летео североисточно, преко Камбоџе и Вијетнама. Међутим на основу радарских (војни и цивилни) података, закључено је да је авион изненада променио курс са севера на запад, тако да је потрага, која је укључивала десетине бродова и авиона, усмерена на Малачки мореуз и Андаманско море (западно од Малезије).

Седам дана након нестанка авиона (15. март 2014. године), откривен је контакт сателита *Inmarsat*-а, али се на основу анализе сигнала није могла утврдити прецизна локација авиона; ипак, утврђено је да се авион могао налазити у области која обухвата регион од Јаве према југу до Индијског океана југозападно од Аустралије, или у области која се протеже на север преко Азије (од Вијетнама до Туркменистана). Затим, област претраге је проширена на Индијски океан југозападно од Аустралије на јужном луку и југоисточну Азију, западну Кину, индијски потконтинент и централну Азију на северном луку. У међувремену, малезијске власти су саопштиле (24. март 2014. године) да се авион срушио у Индијски океан, југозападно од Аустралије [556].

Потрагу за авионом ометала је удаљена локација места несреће. Од 6. априла 2014. године, откривено је неколико акустичних сигнала, за које се сматрало да потичу из регистратора лета *Boeing*-а 777 (или ″црне кутије″) око 2.000 km северозападно од Перта (Западна Аустралија), док је анализом података сателита *Inmarsat*-а детектован и делимичан сигнал из авиона у 08:19, у складу с локацијом акустичних пингова (последњи детектовани 8. априла 2014). Уколико су ови сигнали били са MH370, батерија регистратора лета је вероватно била на крају свог века трајања. Тако, није пронађена ни ″црна кутија″ – кључ за решавање мистерије.

Прва крхотина авиона, тј. *flaperon* (комбинација флапса и елерона/крилца и закрилца) десног крила авиона, пронађена је тек 29. јула 2015. године, на плажи на острву Реунион, око 3.700 km западно од области Индијског океана коју су претраживали Аустралијске власти. До краја 2016. године, пронађено је више од 20 објеката за које је потврђено/верује се да припадају авиону *Boeing*-а 777 (MH370) на обалама Танзаније, Мозамбика, Јужне Африке, Мадагаскара и Маурицијуса. На основу идентификованих делова авиона, сугерисано је да се авион распао, али се није могло утврдити да ли се то догодило у ваздуху, или при удару у воду.

Свакако, оно што је утицало на претрагу од самог почетка, су контроверзе у вези с истрагом нестанка авиона. Малезијска влада је критикована због објављивања контрадикторних информација у првих неколико дана након нестанка авиона и због тога што је у почетку нерадо делила информације са стручњацима из других држава. Званичници који су истраживали нестанак авиона, у децембру 2016. године, након накнадне анализе сателитских података и моделовања океанских струја, закључили да је место потраге било погрешно, и предложили су да се потрага преусмери око 200 миља северније. Међутим, Владе Малезије, Кине и Аустралије (финансијери потраге), већ су донеле одлуку о обустављању потраге за несталим авионом, осим уколико се не појаве експлицитни докази о прецизној локацији авиона. У недостатку информација, које би указале на конкретну локацију, као и новца за финансирање нових истраживања, потрага за авионом MH370 је у јануару 2017. године и званично је завршена.

Малезијска Влада објавила је свој коначни извештај о нестанку лета 370 (јул, 2018), према коме се сматра да је механички квар на авиону веома мало вероватан узрок нестанка авиона, а да је промена путање лета вероватно резултат ручних уноса. Међутим, авио-истражитељи нису могли утврдити узрок нестанка лета 370.

Могући узроци нестанка авиона

Као могући узроци нестанка лета MH370, наведени су:

- механички квар авиона, као и људски фактор, односно самоубиство пилота/члана посаде. На ово последње, упућивало је то што су трансмисије сигнала вероватно биле прекинуте из унутрашњости авиона; међутим, како је саопштено, није уочено/пронађено никакво сумњиво понашање посаде авиона пре лета. Међутим, према једној од теорија узрок несреће може бити самоубиство капетана авиона и чин масовног убиства с предумишљајем [559], на основу чињенице да је био искључен транспондер, да није било покушаја остваривања комуникације (није послата шифра за хитне случајеве), као и да је онај ко је имао контролу маневрисао авионом до његове крајње локације. При томе, према овој теорији, капетан је смањио притисак у авиону, тако да су сви, осим једног од 239 људи на лету 370 вероватно били у несвести – онеспособљени због изненадног смањења притиска. Међутим, без конкретних доказа, и ова тероија је на нивоу спекулација. Ипак, познати су случајеви авио-несрећа узрокованих покушајем самоубиства или самоубиством пилота/копилота, као што је несрећа авиона *Japan Air Lines* (*McDonnell Douglas* DC-8-61), фебруара 1982. године, у којој је 24 особе изгубило живот, а истрага утврдила да је узрок пада авиона – намерна радња капетана (касније је откривено да је капетан боловао од параноидне шизофреније пре инцидента, тако да је проглашен невиним због болести); истражитељи јапанске владе приписали су инцидент недостатку одговарајућих медицинских прегледа који су омогућили капетану да лети [560]. Затим, фатална несрећа авиона *SilkAir* (*Boeing* 737–300), децембра 1997. године, на лету од Џакарте за Сингапур, који је пао у реку Муси (Суматра), у којој је живот изгубило 104 особа. Авио-несрећу су независно истраживали Амерички национални одбор за безбедност у саобраћају (U.S. *National Transportation Safety Board*, NTBA) и Индонежански национални комитет за безбедност у саобраћају (*Indonesian National Transportation Safety Committee*, NTSC). Према NTBA, до пада авиона дошло је због намерних управљачких инпута, ″највероватније од стране капетана″ [561], док према NTSC-у, нису пронађени ″никакви конкретни докази″ који би подржали теорију о самоубиству. Међутим, истражитељи ове авио-несреће открили су да је капетан имао неколико потенцијалних мотива који су претходили авио-несрећи, а који су указивали на његово наводно самоубиство. Осим великих финансијских проблема, имао је и личне сукобе с другим колегама, као и неколико изречених дисциплинских мера у вези са обављањем посла. Свакако, еклатантан пример самоубиства пилота и чин масовног убиства с предумишљајем, јесте фатална несрећа авиона *Germanwings*-а (*Airbus* 320), који је полетео из Барселоне у правцу Дизелдорфа, 24. марта 2015. У овој авио несрећи, копилот *Andreas Lubitz* је искористио одсуство капетана да преузме потпуну контролу над авионом, усмери авион у планине француских Алпа и тако изазове сопствену, и смрт свих 149 путника и чланова посаде. Након несреће, истражитељи су утврдили да је *Lubitz* имао проблеме с видом, несаницом и неким обликом депресије, због чега је користио психотропне лекове, али је ипак у авио-компанији за коју је радио, био у летачком статусу [562].

- На лету 370, у неком тренутку, транспондер је престао да ради (непознато је да ли се покварио или га је неко намерно искључио), што је резултирало продуженим временским периодом у коме уопште није било контакта с авионом, тако да су истражитељи могли само да дају непрецизно време нестанка авиона.
- Губитак сигнала ACARS-а и транспондера, подстакао је и спекулације о неком облику отмице авиона, међутим, ни једна група/појединац није преузела одговорност за напад, а и мало је вероватно да би отмичари усмерили авион ка јужном делу Индијског океана.
- Након открића крхотина авиона, спекулисано је и да је авион намерно оборен, али како нису пронађени гелери ракета или других пројектила, и ова теорија се чини веома мало вероватном.
- Према мишљењу неких стручњака за сајбер безбедност, постоји вероватноћа да су у потенцијалном сајбер нападу на овај авион, који је поседовао најсавременије системе за комуникацију и извештавање, искључени транспондери који дају сигнале локације авиона [6]. До овог закључка се дошло на основу тога што је FAA (2014), захтевала од *Boeing*-а промене у дизајну авиона, наводећи безбедносне разлоге, с обзиром на то да је постојала могућност да су *Boeing*-ови системи за забаву путника у авиону, конектовани с другим, критичним системима авиона.

Безбедносне препоруке/утицај нестанка MH370 на авио-индустрију

Авион *Boeing* 777 (MH370) је последњу ACARS поруку разменио у 1:07:29, док је последња радарска детекција (SSR) била у 1:21:13, као и последња сателитска комуникација у 08:19, 08. марта 2014. године. У прелиминарном извештају Инспектората за ваздушне несреће малезијског Министарсва саобраћаја, неколико месеци након нестанка авиона, дата је препорука ICAO да испита безбедносне предности увођења стандарда за праћење авиона у реалном времену. Подстакнута нестанком MH370, ICAO је усвојила (2016) нове регулативе у циљу спречавања губитка извештавања о позицији комерцијалног авиона, када је авион у ″стању/режиму опасности″ или је у удаљеном ваздушном простору без радарске покривености [563], најпре као препоруку, а од 2021. године, као обавезну регулативу према којој сваки ново-произведени авион мора имати могућност аутономног емитовања сопствене позиције у интервалима од једног минута или мање од минуте, уколико се нађе у поменутом стању.

Нестанак малезијског лета MH370, покренуо је бројна питања у вези са ефикасношћу тада постојеће авио-технологије. Нова технологија која је развијена као одговор на ову трагедију и решавање сличних инцидената у будућности, као и повећању квалитета ваздухопловне индустрије је ADS–B. Иако се не може са сигурношћу тврдити да би сателитски надзор авиона променио све околности у вези с његовим нестанком (као нпр. онемогућавање злонамерног деактивирања транспондера у току лета), свакако би могло утицати на то да контролори лета добију бржу информацију о постојању проблема, као и да потрага за несталим авионом буде много ефикаснија (аналитички, временски и финансијски). И шире, ADS–B надзор у реалном времену, повећава квалитет ваздухопловне индустрије у

целини: омогућава авионима да лете оптималније руте, затим, континуирани интерни пренос податка о локацији и перформансама, географско праћење прекоокеанских летова и у зонама без радарске покривености, као и често ажурирање података. Тренутни ADS–B Out и ADS–B In системи, као што је објашњено у делу 6.1.4., минимизирају опасности и трагедије у авио-саобраћају – пилоти по први пут виде оно што виде и контролори: екране који приказују друге ваздухоплове у ваздуху. Затим, дисплеји у кокпиту прецизно указују на опасне метеоролошке услове и терен, дајући пилотима веома важне информације о лету, као што су привремена ограничења лета. Такође, ослањањем на сателитску навигацију, уместо традиционалних земаљских навигационих средстава, авиони ће имати оптималније руте (авиони ће летети директније), тако штедећи време и новац, истовремено смањујући сагоревање горива и емисије штетних гасова.

Након више од три године од трагедије, *Malaysia Airlines*[198] саопштила је да ће бити прва авио-компанија која ће почети да прати све своје авионе коришћењем мреже сателита, омогућавајући авио-компанијама да континуирано располажу с 100% глобалних података о надзору лета. У прилог томе је и следећа изјава ″Први пут икада, авио-компаније ће моћи да прате своје авионе чак и на местима која не опслужују тренутне сателитске констелације — и није важно да ли лете изнад океана, да ли су изнад пустиње, или изнад Северног пола: знаћемо где је авион″ (*Daniel Baker*, оснивач и извршни директор *FlightAware* -а [554]).

Тренутно, прецизно праћење лета омогућено је мрежом од 66 сателита које је *Iridium,* матична компанија *Aireon*-а (први глобални пружилац услуге за океанско раздвајање авиона), лансирала и поставила у орбиту. На сваком од сателита налази се пријемник који може пратити летове користећи ADS–B технологију, захтевани стандард од 2020. године за летове у већини контролисаних ваздушних простора (FAA) (део 6.1.1).

7.1.2. Фатална несрећа етијопијског *Boeing* 737–800 Max

Генерисање концепта аутономног летења за *e-Enabled* авионе (*Boeing* B787, *Airbus* A380 i A350), увело је нове сајбер ризике (део 3.1.1). О томе сведоче две авионске несреће са фаталним исходима (у којима је укупно **346 особа изгубило живот**), једне, која се догодила 2018. године у Индонезији (погинуло је свих 189 путника), и друге, 2019. године у Етијопији (157 особа је изгубило живот), истог типа авиона – *Boeing* 737 MAX 8 (овај тип авиона је у комерцијалној употреби од 2017. године). Иако су се одређене чињенице и околности у вези са овим авио-несрећама разликовале, заједничко за обе, осим што се ради о истом типу авиона, је и то што су се обе несреће догодиле у истој фази лета авиона (недуго након полетања); при томе, пилоти су пријавили непредвиђену ситуацију, а независни комерцијални сервиси за праћење лета регистровали су девијације у тзв. вертикалној брзини. Тек

[198] Поред нестанка MH370, друга катастрофа, која је погодила *Malaysia Airlines* исте године, је фатална несрећа авиона *Boeing* 777-200 (MH17), на лету од Амстердама (Холандија) до Куала Лумпура (Малезија), који је пао у источној Украјини 17. јула 2014. Свих 283 путника и 15 чланова посаде, погинуло је у овој авио-несрећи, а истрагом је утврђено да је авион оборен ракетом земља–ваздух руске производње.

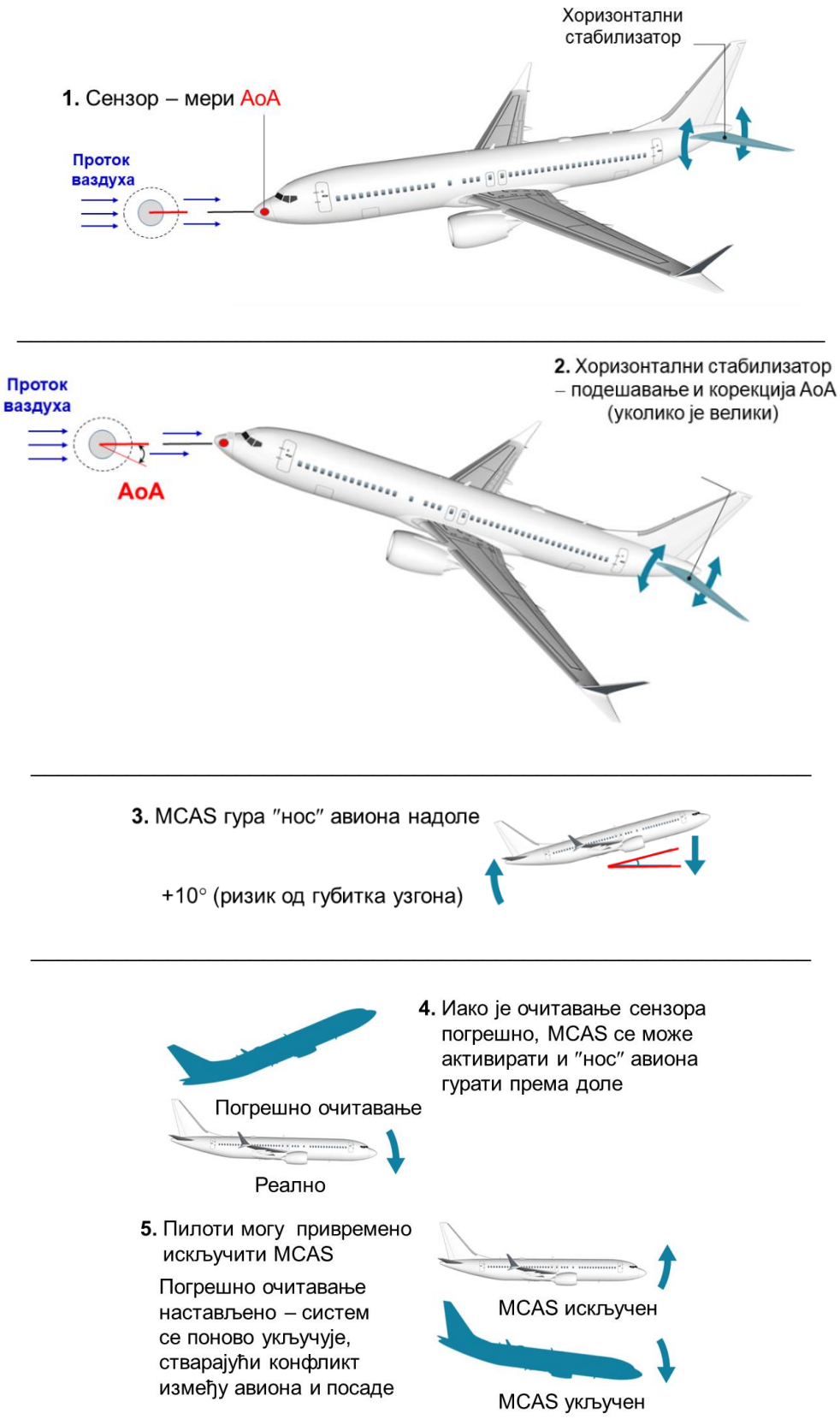
након друге фаталне несреће *Boeing*-а 737MAX 8 (2019), пет месеци након прве несреће овог типа авиона (29. октобар 2018. године) индонежанске компаније *Lion Air*, сви *Boeing*-ови авиони овог типа (више од 300) су приземљени [133], због сумње у безбедност авиона.

Шта је узрок несреће која се догодила шест минута након полетања авиона *Boeing* 737 MAX 8 *Ethiopian Airlines*-а (лет 302)[199], 10. марта 2019, који је летео на редовној линији од Адис Абебе (Етијопија) до Најробија (Кенија)? Прелиминарни извештај (4. april 2019.) [564], указује на то да су погрешни сигнали, које је слао сензор (сл. 44) софтверском систему *Maneuvering Characteristics Augmentation System* (MCAS), а који је требало да стабилизује авион, највероватнији узрок пада авиона. Према извештајима, пилоти су пратили процедуре добијене од стране *Boeing*-а и FAA, и искључили MCAS. Међутим, овај систем је реаговао учестало, чак и када су га пилоти искључили након првог обарања носа авиона. Иако су пилоти покушали да ручно управљају авионом, нису успели да поврате контролу.

Слика 44. Сматра се да је узрок пада авиона *Boeing* 737 *Max* у Индонезији и Етијопији исти – неисправни сензор "нападног" угла (модификовано и преузето из 564])

Како функционише MCAS систем? MCAS је дизајниран (сл. 45) да се активира аутоматски током лета авиона, када су закрилца (флапсови) у позицији UP и при већим "нападним" угловима (*Angle of Attack*, AoA). Нападни угао, AoA представља угао између тетиве аеропрофила и релативног ветра, тј. протока ваздуха (сл. 45 а).

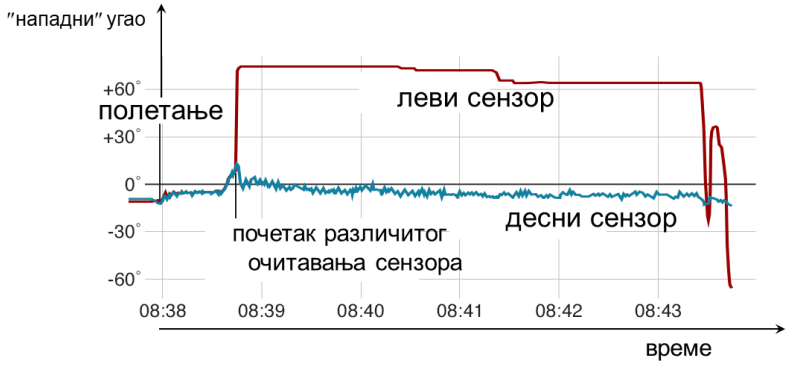
[199] Ова несрећа етијопијског авиона на лету 302 (2019), превазишла је, по броју жртава, до тада највећу авио несрећу *Ethiopian Airline* (лет 961), изазвану отмицом авиона, тј. незаконитим активностима отмичара, што је довело до губитка потиска мотора услед недостатка горива, и резултирало падом авиона у близини Коморских острва (1996). У овој авионској несрећи живот је изгубило 119 путника и свих 6 чланова посаде [565].



Слика 45. Функционисање *Maneuvering Characteristics Augmentation System* (MCAS) (модификовано и преузето из [564])

Поједностављено, MCAS систем, у случају када је AoA велики, аутоматски обара "нос" авиона, тј. доводи авион у "нормалну позицију лета", како би се избегао губитак узгона (*stall*). MCAS понавља поступак, уколико идентификује да је AoA (сл. 45) и даље велики. Вредност AoA добија се од једног сензора, и уколико је овај угао погрешно очитан, MCAS се може активирати, и гурати нос авиона надоле

Иако се у извештају етијопијских власти, MCAS не помиње експлицитно, истиче се да су пилоти имали проблем са контролом AOA и да је сензор давао погрешне податке (сл. 46). Искључивање MCAS система, приказано је на сл. 47.



Слика 46. Различита очитавања сензора (левог и десног) етијопијског авиона *Boeing* 737 MAX 8 (модификовано и преузето из [564])

Слика 47. Искључивање *Maneuvering Characteristics Augmentation System* (MCAS) (модификовано и преузето из [564])

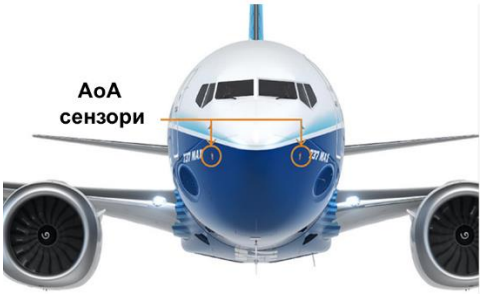
Чињенице и коментари

На основу извештаја, ситуација у кокпиту авиона Boing 737 MAX 8 (ETH302), 10. марта 2019. године, била је следећа [564]:

08:38 – лажно показивање сензора да је авион близу столинга; MCAS се аутоматски покреће и гура ″нос″ авиона надоле
08:39–40 – пилоти предузимају контрамере: подешавањем угла на репном стабилизатору авиона користећи електричне прекидаче на волану, покушавају да врате нос авиона нагоре
08:40 – пилоти искључују електрични систем који напаја струјом компјутер/софтвер, а који гура ″нос″ авиона надоле

На основу извештаја FAA и етијопијског одбора за националну безбедност у саобраћају, а на основу доказа прикупљених са места несрећа и сателитких података, закључује се да су оба лета авиона *Boeing* 737 MAX ″била веома слична″. Ипак, иако је компанија *Boeing*, након прве авио несреће, 2018. године, издала смернице пилотима о управљању MCAS-ом, неопходне измене у софтверу, одлагане су више пута. Такође, амерички експерти за безбедност у ваздухопловству, као и регулатори, показивали су скепсу према тврдњама FAA и *Boeing*-а о безбедном функционисању MCAS-а, као и обученошћу пилота за његово коришћење. На пример, тест пилоти у симулираном лету *Lion Air*-а, установили су да пилоти имају мање од 40 s да реше проблем неповратног понирања авиона.

Коначно, према документу из марта 2019. године (*U.S. Department of Transportation Office of Inspector General*) [566], FAA је одговорна за надзор и сертификацију свих цивилних авиона произведених у USA. Иако је FAA задржала висок безбедносни ниво, несреће авиона *Boeing* 737 Max, у октобру 2018. и марту 2019, изазвале су велику безбедносну забринутост. Ове несреће, указале су на суштински недостатак MCAS, што је резултирало изменом софтвера увођењем додатног сензора (сл. 48), и у вишој истанци – ревизијом комплетног процеса FAA сертификације авиона [567]. Ипак, авио несрећа у Етијопији била је ″кап која је прелила чашу″, а више од 400 пилота [568], који су летели на *Boeing*-у 737 Max туже произвођача, оптужујући компанију *Boeing* да коорпоративни профит ставља изнад авио безбедности ″невиђеним прикривањем познатих недостатака у дизајну авиона″.



Слика 48. Након приземљења авиона типа *Boeing* 737 Max, компанија *Boeing* ажурира софтвер MCAS-а и уводи још један AoA сензор (модификовано и преузето из [569])

Безбедносне препоруке

На конференцији за штампу, у Њујорку (август, 2019. године) [570], најављен је повратак *Boeing* 737 MAX 8 за 2019. годину, као и истакнуто да компанија *Boeing* блиско сарађује са FAA и другим ентитетима у отклањању недостатака MCAS-а. Међутим, начин на који је овај систем одобрен, а који је омогућио *Boeing*-у да самостално сертификује многе системе, изазазвали су оштре критике *Boeing*-а, као и FAA, која није приземљила авионе типа *Boeing* 737 MAX 8 након прве несреће у октобру 2018. У вези с тим, компанија *Boeing* је потенцирала да разуме незадовољство, као и да разуме да ће бити потребно време да поново стекне поверење јавности.

Након ригорозног тестирања, 2021. године, власти цивилног ваздухопловства многих држава у свету, одобриле су да се *Boeing* 737 MAX 8 "врати на небо", укључујући USA, Канаду, UK, Аустралију, Бразил и EU. Међутим, Кина, друго по величини светско тржиште за комерцијални ваздушни саобраћај, и даље забрањује коришћење овог типа авиона. Према изјавама кинеских власти за цивилно ваздухопловство и регулатора, разматра се планирање тестирања овог типа авиона, и истиче да ће се тестови за сертификацију спроводити корак по корак, када се реше главни безбедностни проблеми постављени *Boeing*-у [571].

Слика 49. Приказ примарних информација о лету потребних за безбедно и ефикасно управљање 737 MAX; AoA индикатор даје додатне информације посади авиона (модификовано и преузето из [569, 572])

Компанија *Boeing* је развила ажурирање софтвера MCAS у циљу обезбеђивања додатних слојева заштите уколико AoA сензори пошаљу погрешне податке. Софтвер је прошао много часова анализа, лабораторијског тестирања, верификације на симулатору и бројних пробних летова, као и валидиран током сертификационих тестова у лету са представницима FAA [569]. Поменути додатни слојеви заштите укључују следеће: FCS (*Flight Control System*) упоређује податке добијене са два AoA сензора. Уколико постоји неслагање од 5,5° или више, с увученим флапсовима, MCAS се неће активирати. Индикатор на екрану пилотске кабине (сл. 49) даје упозорење пилотима. Аутоматски систем, ни у ком случају, не може направити толико велики захтев на управљачку површину хоризонталног стабилизатора, да се она не би могла надјачати мануелним путем. Пилоти и даље имају могућност да "заобиђу" MCAS и ручно контролишу авион. Очекује се да ће

ова ажурирања смањити оптерећење посаде у проблематичним ситуацијама лета и спречити ситуацију у којој погрешни подаци доводе до активирања MCAS-а. Поред тога, *Boeing*-ова обука пилота, која укључује нови пакет рачунарских модула за обуку, нову и ажурирану документацију и обуку на симулатору, дизајнира је тако да омогући боље разумевање FCS-а и проширивање техничког знања пилота, као и да поврати поверење у *Boeing* 737 MAX.

7.3. ПРИМЕРИ ПРИМЕНЕ ADS–B У ВАЗДУШНОМ САОБРАЋАЈУ

Нестанак (2014) малезијског авиона *Boeing* 777 (MH370), као што је описано у делу 7.2.1., унапредио је дискусију о ADS–B и реалној потреби за увођењем напреднијих алата за надзор авиона. Ова напредна технологија која се користи у савременим авионима и која аутоматски преноси нешифровану идентификацију и стање авиона у веома кратким временским интервалима (од < 1 s, до неколико секунди), обавезни је стандард у цивилној авијацији од 2022. године. Приступачност ADS–B пријемника омогућава праћење ваздушног саобраћаја, као и формирање онлајн мрежа пријемника који сервирају податке онлајн сервисима (и комерцијалним и бесплатним). Тако, експоненцијално растућом количином података за анализу, омогућава се решавање многих сложених проблема у пракси, као што је детаљна анализа инцидентних ситуација у авијацији. На пример, *Learjet* је учествовао у фаталној несрећи (децембар 2021. године) на *Gillespie Field*-у (*El Cajon, California*) [573]. Према прелиминарном извештају USA *National Transportation Safety Board* (NTSB), како се може сагледати из ADS–B података, прилаз авиона није био стабилан, док је пилот покушавао да слети из процедуре кружења. Затим, према ADS–B подацима и релевантним информацијама о положају, прелиминарни извештај NTSB –а, који се односи на фатални судар у ваздуху између B-17G и P-63F *Kingcobra* (регистрованог у *American Airpower Heritage Flying Museum*) током аеромитинга у Даласу (новембар 2022.), показали су није било раздвајања авиона [574]. Метеоролошки услови у тренутку несреће, у којој је живот изгубило 6 особа, били су повољни; оба авиона су била опремљена ADS–B-ом и GPS-ом. Поред тога, B-17G имао је *Avidyne* IFD540, а GPSMap 496 из авиона није забележио никакве информације о лету. Коначни извештај о овој несрећи тек треба да буде објављен.

Широке могућности које нуди ADS–B описане су на следећим примерима: Фатална несрећа кинеског авиона *Boeing* 737–800 (март, 2022) (део 7.3.1); Девијација путање лета *United Airlines*-а (децембар, 2022) (део 7.3.2); Понирање током процедуре полетања лета *Boeing* 787-8 *Qatar Airways*-а (јануар, 2023) (део 7.3.3).

7.3.1. Фатална несрећа кинеског авиона *Boeing* 737–800 (март, 2022)

На редовној линији авиона *Boeing* 737–800 (B-1791, лет MU5735), 21. марта 2022. године, од *Kunming*-а (Кина) за *Guangzhou*-а (Кина), након нешто више од једног часа лета, авион је изненада прешао с висине крстарења у вертикално понирање и ударио у обронак планине јужне кинеске провинције *Guangxi*. У овој авио-несрећи живот је изгубило свих 123 путника и 9 чланова посаде.

Чињенице

Према прелиминарном извештају [575] кинеског регулаторног тела за цивилно ваздухопловство[200] (који садржи чињеничне податке и не садржи анализу или закључке у вези са узроком несреће), посада авиона и техничко особље су испунили релевантне стандарде, имали су важећи сертификат о пловидбености авиона, затим, у авиону није било предмета који би представљали опасност, а метеоролошки услови за обављање лета били су повољни. Пре него што је авион напустио висину крстарења, радио комуникација између посаде и ATC није показала никакве абнормалности. Авион је ушао у зону под радарском контролом *Guangzhou*-а у 14.17 h. Радар обласне контроле упозорио је на девијацију у 14.20.55, а авион је напустио висину крстарења од 8.900 m. ATC је реаговала, али није добила одговор. У 14:21:40, последња информација о авиону, забележена радаром била је: висина према стандардном притиску 3.380 m, путна брзина 1.010 km/h и правац лета (курс) од 117°. Након тога, према извештају, радарски сигнал је нестао. Нађене су две црне кутије (веома оштећене), а прикупљање података и анализа су у току.

Коментар

У односу на друга конвенционална земаљска радио-навигациона средства, као што је истакнуто у делу 6.1.4, ADS–B нуди више оперативних могућности, као што су ADS–B In апликације, детекција конфликта, као и активности тражења/спашавања. Допринос овом последњем, базираном на ADS–B подацима, показао се веома значајним, као нажалост, у овој авио-несрећи. Иако није једино средство које помаже лоцирању места пада авиона, из ADS–B података емитованих из авиона, може се једноставније и брже реконструисати коначна путања.

На примеру ове авио-несреће можемо потпуније сагледати широке могућности онога што ADS–B систем омогућава. Наиме, *FlightRadar24* је прикупио ADS–B податке [576], који су стримовани директно с рачунара авиона током лета. Тачније, последња пријављена ADS–B порука, на основу *AirNav RadarBox* података [577] била је у 06:22:36 (UTC) и вертикална брзина од –32,640 ft/min, која је указивала на то да је авион пао (Табела 13).

Такође, треба нагласити да се из ових ADS–B података могло јасно уочити географска дужина и ширина, како би се реконструисала путања спуштања и прецизније идентификовало место пада авиона. У табели 13, дати су само подаци који се односе на временски интервал од 05:16:46 до 06:22:36 UTC.

---

[200] Према Конвенцији о међународном цивилном ваздухопловству, прелиминарни извештај о истрази, потребно је доставити ICAO и државама које учествују у истрази у року од 30 дана од дана несреће.

Табела 13. Авио-несрећа *China Eastern Airlines*-овог авиона *Boeing* 737–800 (B-1791, лет MU5735): пријављење ADS–B поруке, према *AirNav RadarBox*-у[577]

Време	LAT	LONG	Курс (°)	Алтитуда (ft)	GS (kts)	VR (fpm)	SQUAWK
05:16:46 UTC	25.0929	102.9101	↙ 221	8225	178	↗ 2560	2101
05:17:46 UTC	25.0542	102.8599	↙ 232	9350	249	↗ 896	
05:18:46 UTC	25.0056	102.8072	↙ 197	12325	259	↗ 3712	
05:19:46 UTC	24.9404	102.8548	↘ 146	14475	346	↗ 2560	
05:20:46 UTC	24.8978	102.9512	↘ 116	17325	353	↗ 2752	
05:21:46 UTC	24.8525	103.0513	↘ 115	19025	382	↗ 2880	
05:22:46 UTC	24.7962	103.1513	↘ 141	21050	384	↗ 1472	
05:23:46 UTC	24.6983	103.1967	↘ 158	22950	396	↗ 2240	
05:24:46 UTC	24.6055	103.2646	↘ 134	24800	418	↗ 1856	
06:00:46 UTC	23.7387	108.1344	→ 093	29100	461		
06:02:48 UTC	23.7227	108.4190	→ 093	29100	461	64	
06:05:45 UTC	23.6998	108.8146	→ 093	29100	458	64	
06:17:45 UTC	23.4143	110.4491	↘ 100	29100	454		
06:19:45 UTC	23.3702	110.7202	↘ 100	29100	457		
06:20:45 UTC	23.3479	110.8558	↘ 100	29100	457		
06:21:45 UTC	23.3149	110.9834	↗ 081	7850	590	↘ –15744	
06:22:36 UTC	23.3375	111.1056	↗ 087	3225	376	↘ –32640	

LAT – латитуда; LONG – лонгитуда; ALT – алтитуда у ft AMSL (*above mean sea level*) – висина изнад средњег нивоа мора, 1 ft = 0,3048 m; GS – путна брзина (g*round speed* у kts; 1 kts = 1,852 km/h.); вертикална брзина (*vertical rate*, чији је индикатор тзв. "инструмент за диференцијални притисак"; јединица за VR је fpm, *feet per minute*); SQUAWK –посебан SSR кôд транспондера додељен авиону (фуснота 73)

7.3.2. Девијација путање лета UA1722 (децембар, 2022)

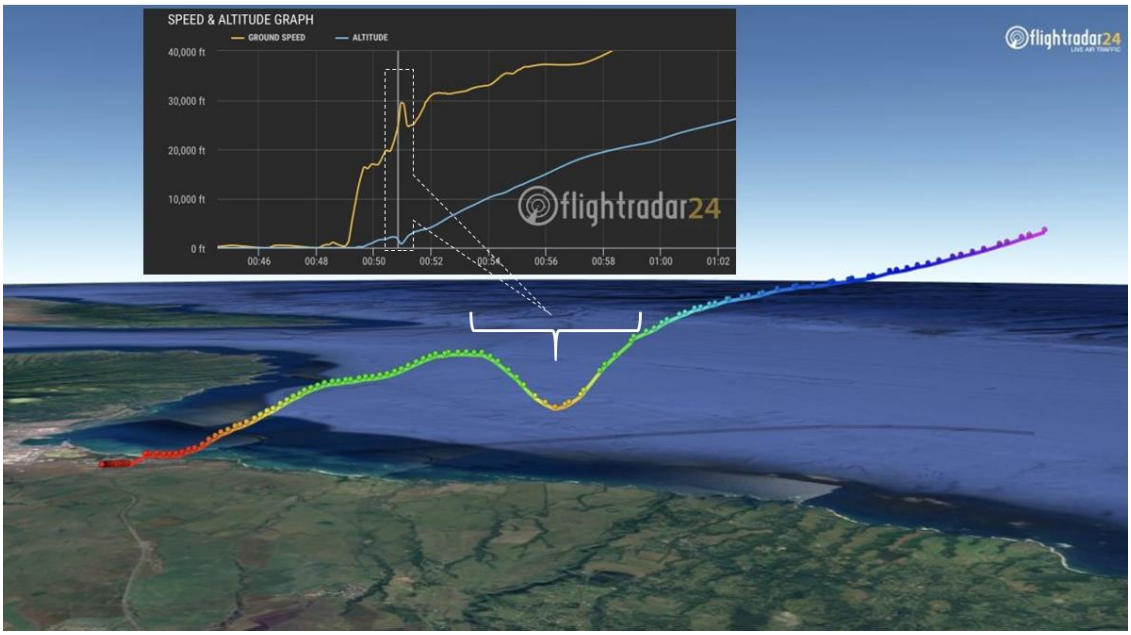
Авион (*Boeing* 777–200ER, N212UA), лет UA1722 (18. децембар 2022) од *Kahului* (*Hawaii*) за *San Francisco* (USA) је нормално полетео, а након 71 s, прешао u понирање. У овом авио-инциденту, није било повређених путника.

Авион *Boeing* 777–200ER, лет UA1722 полетео је у 00:49.28.882 UTC, 19. децембра 2022. (18. децембар у 14:49, по локалном времену). У 00:50:39.007, попео се на висину од 2200 ft, а након тога, у 00:50:57.500 је изгубио висину, тј. спустио се на 775 ft (сл. 50). Затим, авион се стабилизовао, наставио пењање и безбедно стигао у *San Francisco* у 05:03 UTC. Prema *The Air Current*, инцидент је пријављен авио-компанији након слетања, о чему је обавештена и FAA.

Одступање од путање, емитовано је и може се анализирати на основу података добијених од ADS–B система. ADS–B податке обезбеђује *Flightradar*24, а доступне су три различите датотеке – стандардне CSV и KML датотеке, као и грануларни CSV. Прва два фајла (стандардна CSV и KML датотека) обухватају стадардне податке за цео лет, док грануларни CSV садржи само податке који се односе на полазну фазу лета (*departure*). Генерално, сваки CSV (*Comma Separated Values*) фајл, садржи податке о времену, позицији и кретању. То је CSV табела са 6 колона

– прва колона садржи временске податке (UTC формат)[201], друга колона садржи позивни знак лета (тро-словни ICAO идентификатор авио компаније), трећа колона садржи податке о позицији (приказане као латитуда и лонгитуда, тј. географска ширина и дужина), док последње три колоне садрже податке о висини (алтитуда у ft AMSL[202]), брзина (путна брзина у kts[203]) и смер (*heading*). За приказ географских података у програмима, као што је *Google Earth*, користе се KML (*Keyhole Markup Language*) датотеке, које омогућавају четворо-димензионо приказивање података о лету. KML датотеке су веома корисне за поређење путања летова истог авиона (у различитим временским периодима), различитих типова авиона истог броја лета и сл; подаци из фајлова могу се комбиновати, чувати и по потреби користити за будуће анализе [578].

Скуп ADS–B података које је обезбедио *Flightradar*24 (грануларни CSV) дат је у табели 14. Конкретно, скуп података приказан у табели 14, односи се само на део путање, тј. на фазу лета у којој је авион достигао око 2200 ft, затим ушао у понирање достижући висину од 775 ft, а након тога, поново почео да се пење (део путање лета означен је витичастом заградом на сл. 50).



Слика 50. Мапа и путања лета *United Airlines*-а (лет UA1722), 18. 12. 2022. добијени на основу ADS–B података. Уметнута слика: графици брзине и надморске висине (слика модификована и преузета из [579])

[201] UTC формат садржи 2 цифре за час на основу 24-часовног сата, након чега следе две цифре за минуте и две цифре за секунде, раздвојене двотачкама.
[202] ft AMSL (*above mean sea level*) – висина изнад средњег нивоа мора; 1 ft = 0,3048 m.
[203] kts (Чвор) – јединица за путну брзину; 1 kts = 1,852 km/h.

Табела 14. Лет UA1722, авиона *Boeing* 777-200EP, *United Airlines*-а: пријављене ADS–B поруке, које обухватају временски период 00:50:37:759–00:51:11:250 UTC према *Air Current*-у [579]

Time	LAT	LONG	ALT (ft AMSL)	GS (kts)	Track	VR (fpm)	Receiver	GPS Alt (ft)
00:50:37Z.759	20.94413	–156.402	2175	203	30	576	1521	GPSA:2150
00:50:39Z.007	**20.94478**	**–156.401**	**2200**	**208**	**30**	**192**	**40218**	**GPSA:2175**
00:50:40Z.389	20.9464	–156.4	2200	210	30	–64	1521	GPSA:2175
00:50:42Z.005	20.94786	–156.399	2200	216	31	–384	40218	GPSA:2175
00:50:43Z.775	20.94919	–156.399	2175	222	31	–1216	1521	GPSA:2125
00:50:45Z.029	20.95051	–156.398	2175	227	31	–2112	40218	GPSA:2100
00:50:46Z.659	20.952	–156.397	2075	230	31	–4224	1521	GPSA:2075
00:50:48Z.084	20.9533	–156.396	1950	238	31	–5888	40218	GPSA:1925
00:50:49Z.965	20.95516	–156.395	1725	246	31	–7168	1521	GPSA:1675
00:50:51Z.409	20.95661	–156.394	1550	252	31	–8192	40218	GPSA:1575
00:50:52Z.640	20.95789	–156.393	1350	259	30	–8576	1521	GPSA:1400
00:50:54Z.499	20.95996	–156.392	1075	273	29	–7680	40218	GPSA:1050
00:50:55Z.965	20.96191	–156.391	900	287	28	–5184	1521	GPSA:900
00:50:57Z.500	**20.96373**	**–156.389**	**775**	**295**	**28**	**–2304**	**40218**	**GPSA:825**
00:50:59Z.170	20.96568	–156.388	825	300	28	2816	1521	GPSA:825
00:51:00Z.197	20.9664	–156.388	875	300	28	3712	40218	GPSA:875
00:51:01Z.680	20.96862	–156.387	1050	294	29	7168	40218	GPSA:1025
00:51:02Z.245	20.96919	–156.386	1150	286	29	7744	1521	GPSA:1150
00:51:05Z.237	20.9722	–156.384	1625	256	30	8640	1521	GPSA:1575
00:51:06Z.245	20.97318	-156.384	1775	247	29	8128	40218	GPSA:1700
00:51:08Z.196	20.9751	–156.383	2000	248	29	7168	1521	GPSA:1925
00:51:11Z.250	20.97821	–156.381	2350	247	30	5760	1521	GPSA:2275

LAT – латитуда; LONG – лонгитуда; ALT – алтитуда у ft AMSL (*above mean sea level*) – висина изнад средњег нивоа мора, 1 ft = 0,3048 m; GS – путна брзина (*ground speed* у kts; 1 kts = 1,852 km/h); VR – вертикална брзина (*vertical rate*, чији је индикатор тзв. ″инструмент за диференцијални притисак″; јединица за VR је fpm, *feet per minute*); *track* (путања) – добија се као корелација, коришћењем посебног алгоритма (праћења) низа радарских пријављених позиција за један авион; извештај најчешће садржи фино подешене (″глатке″) информације о позицији и вектору брзине;

У овом описаном случају, узроци девијације у путањи, могу бити метеоролошки услови. Као што је познато, на путању лета утичу атмосферски/метеоролошки услови, асиметрија авиона, отказ мотора у вишемоторним авионима, асиметрично

постављен терет, изненадна оштећења током лета (удар птица, град и сл.). Стога је веома значајно одредити границе у оквиру којих се обавља безбедан лет, а који се базира на поређењу постојећег/расположивог и захтеваног отклона контролних површина. У те сврхе предлаже се метода заснована на овим захтеваним помацима контроле лета (који се односе на захтеве маневрисања и на оне који су потребни за компензацију бочног ветра као и било које врсте асиметричног оптерећења авиона) у комбинацији с нумеричким симулацијама [580–583]. Поред тога, овај релативно једноставан и робустан метод примењљив је на анализу случајева асиметричног оптерећења авиона како у редовној употреби тако и у стању отказа.

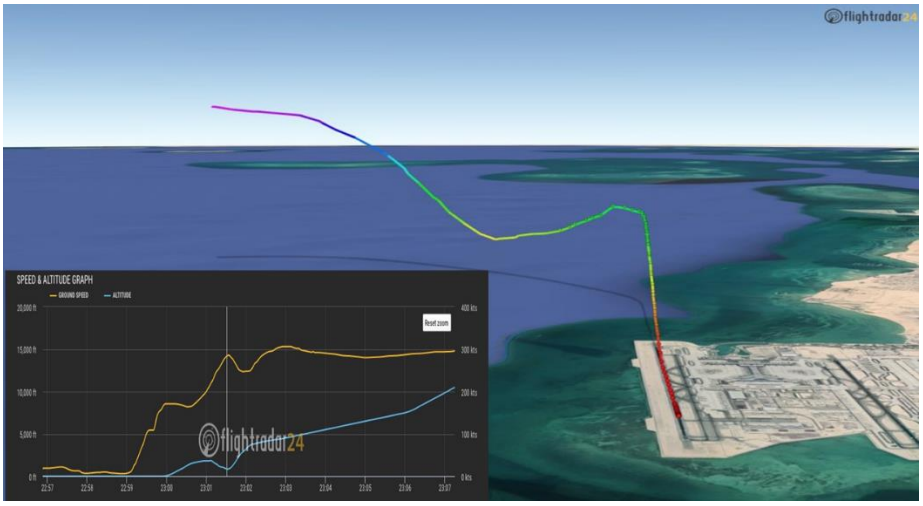
Свакако, из података ADS–B могу se добити квантитативне информације које су инхерентно повезане са динамиком авиона и стога се могу користити за поређење са предвиђањима динамичког модела. Односно, ADS–B пружа фино подешавање параметара који омогућава праћење секвенце путање авиона, а која одговара одређеним фазама лета.

7.3.3. Понирање током процедуре полетања авиона *Boeing* 787-8 (QR161) (јануар, 2023)

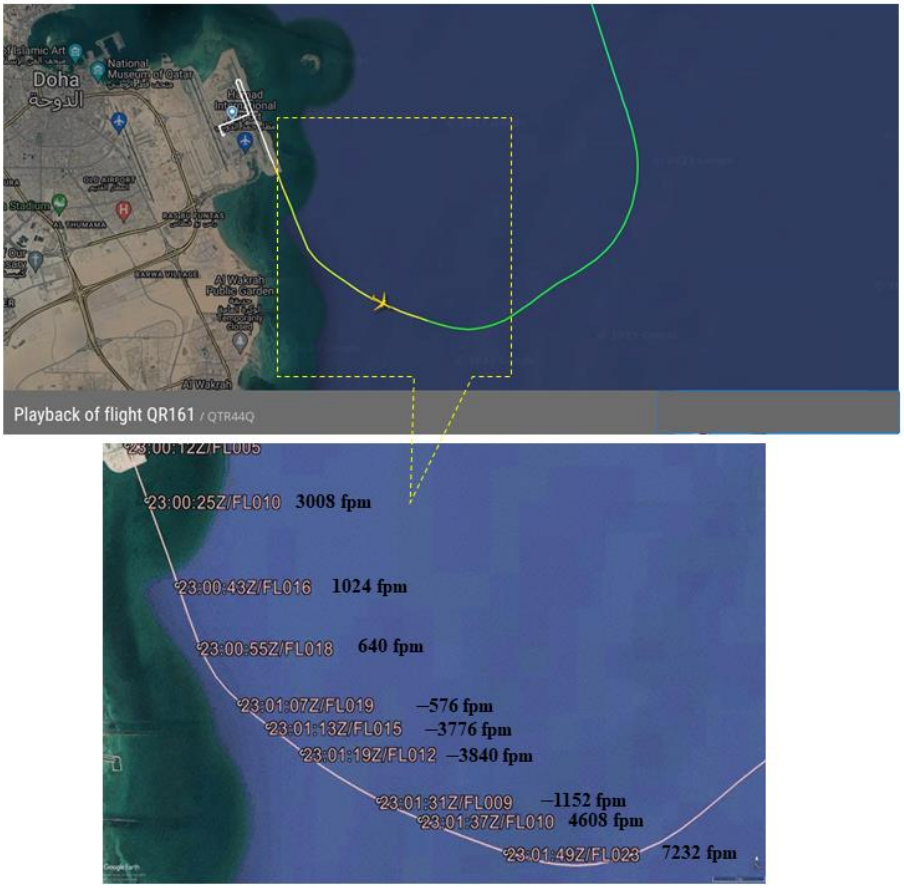
У недавном инциденту (10. јануар 2023. године), авион *Boeing* 787-8 (A7-BCO) *Qatar Airways*-а (лет QR161), на лету од Дохе (Катар) до Копенхагена (Данска), је убрзо након полетања (за мање од два минута), прешао из фазе пењања у нагло понирање, након чега се стабилизовао, наставио пењање и шест часова касније, безбедно стигао у Копенхаген. У овом авио-инциденту, није било повређених путника. *Qatar Airways* је дао саопштење у коме се наводи да је компанија упозната са догађајем који се односи на лет QR161, да је исти одмах пријављен властима, затим, да је у току интерна истрага (у складу са најстрожим стандардима безбедности, обуке и извештавања), као и да се ради на корективним поступцима у складу са стандардима авио-индустрије.

Авион *Boeing* 787–8 (лет QR161) полетео са писте међународног аеродрома Хамад у ноћним условима, у 22:59:58Z.737 UTC. Током пењања, у 23:01:04Z.864, достигао је висину од 1850 ft AMSL. Затим, током левог заокрета (са 157° на око 100°), авион је прешао у понирање, спустивши се на само 800 ft AMSL у 23:01:33Z.374 (сл. 51). У периоду од 28 секунди, авион се спуштао, изгубивши 1000 ft висине и достигавши вертикалне брзине веће од –3000 fpm (сл. 52). Након тога, авион се стабилизовао и наставио лет за Копенхаген.

Понирање авиона током процедуре полетања, емитовано је и може се анализирати на основу података добијених од ADS–B система. Скуп ADS–B података које је обезбедио *Flightradar24* (грануларни CSV) дат је у табели 15. Конкретно, скуп података приказан у табели 15, односи се само на део путање, тј. на фазу лета у периоду од 53 s (временска секвенца од 23:01:18Z.082 до 23:02:11Z.298) у којој је авион након достизања максималне алтитуде, од 1850 ft, спустио на 1275 ft (вертикална брзина –3840 fpm), а затим на 800 ft (вертикална брзина –64 fpm), а затим поново прешао у режим пењања (сл. 52).



Слика 51. Мапа и путања лета *Qatar Airways*-а (лет QR161), 10. јануар 2023. године, добијени на основу ADS–B података. Уметнута слика: графици брзине и висине (слика модификована и преузета из [584]



Слика 52. Мапа и путања лета *Qatar Airways*-а (лет QR161), 10. јануар 2023. године (графика: AVH/*Google Earth* (слика модификована и преузета из [584])

Табела 15. Лет QR161, авиона *Boeing* 787–8, *Qatar Airways*-а: пријављене ADS–B поруке, које обухватају временски период 23:01:18Z.082–23:02:11Z.298 UTC на основу грануларног CSV-а (*Flightradar*24) [585]

Временска ознака	Латитуда	Лонгитуда	Алтитуда (ft AMSL)*	GS** (kts)	Путања***	VR**** (fpm)
23:01:18Z.082	**25.2084**	**51.65934**	**1275**	**252**	**124**	**–3840**
23:01:28Z.465	25.20175	51.67171	950	279	117	–1856
23:01:29Z.308	25.20145	51.67236	900	281	116	–2240
23:01:32Z.308	25.19962	51.67653	825	285	114	–1152
23:01:33Z.374	**25.19938**	**51.6772**	**800**	**287**	**113**	**–64**
23:01:35Z.418	25.19798	51.68098	900	286	112	1536
23:01:38Z.421	25.19798	51.68488	1125	280	110	4608
23:01:38Z.836	25.19645	51.68554	1175	280	110	4608
23:01:41Z.188	25.19545	51.68859	1375	273	109	5952
23:01:43Z.752	25.19463	51.69118	1650	268	109	6656
23:01:44Z.270	25.19421	51.6925	1725	265	108	6912
23:01:47Z.376	25.19307	51.69627	2075	257	108	7232
23:01:49Z.108	25.19238	51.69871	2275	254	107	7232
23:01:50Z.312	25.19215	51.69973	2425	250	106	7104
23:01:53Z.281	25.19119	51.70364	2725	248	103	5696
23:01:54Z.402	25.19096	51.70486	2800	248	102	5312
23:01:59Z.597	25.19019	51.71138	3175	247	94	4352
23:01:59Z.645	25.19019	51.71138	3175	247	94	4352
23:02:02Z.588	25.1903	51.71555	3375	248	86	4480
23:02:04Z.728	25.19069	51.71819	3550	248	81	4416
23:02:05Z.250	25.19081	51.71881	3600	249	79	4224
23:02:08Z.574	25.19165	51.72255	3750	254	74	2560
23:02:09Z.916	25.1922	51.72445	3775	256	73	1856
23:02:11Z.298	25.19289	51.72643	3800	260	69	1024

*ft AMSL (*above mean sea level*) – висина изнад средњег нивоа мора; 1 ft = 0,3048 m
**GS (*ground speed*) – путна брзина; јединица за GS је kts (чвор); 1 kts = 1,852 km/h
***Путања (*track*) – добија се као корелација, коришћењем посебног алгоритма (праћења) низа радарских пријављених позиција за један авион; извештај најчешће садржи фино подешене (″глатке″) информације о позицији и вектору брзине
****VR (*vertical rate*) – вертикална брзина; јединица за VR је fpm (*feet per minute*) чији је индикатор тзв. инструмент за диференцијални притисак

Због чега се догодио овај инцидент и зашто је авион изгубио 1000 ft висине током критичне фазе лета, при чему су метеоролошки услови били више него добри? Прелиминарно, узрок овог инцидента, који је био веома близу катастрофе, јесте људски фактор. Наиме, копилот (који је био пилот који лети) је изгубио свест о ситуацији и превео авион у понирање. Након тога, капатан је преузео команде и стабилизовао авион и вратио га на захтевани профил лета.

ЗАКЉУЧАК

Од почетка 21. века, авијација пролази кроз константни процес трансформације с применом нових ICT у земаљским, ваздушним и свемирским системима, а током протеклих година, поред значаја сигурности у цивилном ваздухопловству, не може се пренебрегнути и значај сајбер безбедности у сектору ваздухопловства. У складу са основном хипотезом истраживања, **модернизација авио-система**, као што је еволуција земаљске контроле ваздушног саобраћаја у ону засновану на сателитским контролним системима с бројним комуникационим везама и услугама, као што је прелазак на ADS–B (*Automatic Dependent Surveillance – Broadcast*) бежични комуникациони протокол, **креира критичне рањивости** и захтева значајан пораст свести о питањима сајбер безбедности. Дакле, једино **пораст безбедности** и **подизање нивоа свести** у сектору цивилне авијације, на нивоу држава, као и глобално, омогућава спречавање/минимизирање експлоатације постојећих рањивости у будућности.

Увођење **ADS–B**, мултипараметарског система за надзор, као глобалног стандарда у комерцијалном ваздухопловству, представља **гигански корак** у **модернизацији** и **побољшању квалитета** ваздухопловних операција. Дизајниран је у циљу унапређења кључних сегмената ваздушног саобраћаја – омогућавање надзора у реалном времену, повећања безбедности и ефикасности, као и побољшање информација о лету и метеоролошких података. ADS–B систем подржава две различите услуге, **ADS–B Out** (аутоматски преноси параметре лета авиона из авиона до ATC на Земљи) и **ADS–B In** (омогућава пријем ADS–B информација од других авиона у близини); функција ADS–B In значајно побољшава свест пилота о ситуацији, омогућавајући приступ готово идентичним подацима које су на располагању ATC оператерима на Земљи. Иако само комплетан систем ADS–B Out/In пружа бројне предности (додатну свест о ситуацији, ефикасније океанске руте, итд.), FAA и EASA захтевале су потпуну имплементацију ADS–B Out, при чему ADS–B In остаје опциона услуга из неколико разлога, као што су трошкови имплементације, различити стандарди опреме и захтеви за кокпит. Према финалној одлуци ових организација, крај временског рока за имплементацију ADS–B Out била је 2020. година, а затим 2022. година (ADS–B је сада обавезан у Америци, Аустралији и Европи). Свакако, **2020. година** ће остати упамћена као **значајна преломна тачка у историји ваздухопловства**, и то не само због поменутог мандата ADS–B-а, већ и као година у којој је пандемија (Covid-19), изазвала тектонске промене у авијацији, генерално, драстично смањивши промет путника на глобалном нивоу, као и имобилишући бројне авионе.

Иако егзистирају бројне апликације и **предности коришћења ADS–B података**, постоји реална **забринутост** да се ова врста података/информација може погрешно применити/злоупотребити. Због тога је увођење ADS–B у авијацији, као нове технологије, праћено изазовима, па чак и одређеном врстом скепсе. Наиме, **недостатак фундаменталних безбедносних механизама**, као што су енкрипција и аутентификација, уводи безбедносне пропусте који се могу искористити од стране различитих злонамерних хакера. Конкретно, на ADS–B систем могу се извршити различити **бежични сајбер напади**, као што су **прислушкивање** (*eavesdropping*), **ометање** (*jamming*), убацивање порука, тј. **спуфинг** (*message injection*, тј. *spoofing*),

брисање поруке (*message deletion*) и **модификација поруке** (*message modification*). Ови напади имају различите нивое утицаја (штетног) на авио системе, а напад који може значајно деградирати ваздухопловни систем је напад лажирања (спуфинг) у коме се у пријемник ″жртве″ убацују/подмећу лажни сигнали у циљу погрешног позиционирања или временског одређења. Због свега тога, анализа и развој ефикасних против-мера, тј. метода за детекцију и ублаживаање сајбер напада на ADS–B, предмет је интересовања бројних истраживача и стручњака из области авијације, у циљу повећања сигурности и безбедности система ваздушног саобраћаја. Оваква истраживања су неопходна, с обзиром на то да и пилоти, као и контролори летења доносе веома важне одлуке на основу инструмената, а да погрешна одлука може имати несагледиве последице. Због тога је веома важно анализирати утицај потенцијалних сајбер напада на ADS–B, која је свакако технологија будућности, с бројним бенефитима, а чији је посебан значај наглашен доделом посебне категорије 21 ASTERIX протокола за размену информација о ваздухопловима (EUROCONTROL). Оно што ће омогућити употребу ADS–B технологије равноправно с постојећим авио системима, је **стандардизација** и **унификација хардвера**, као и **софтвера**, а посебно **комуникационих система**. Нарочито, а с обзиром на то да будућност авијације у највећем уделу, следи правац аутоматизоване комуникацији у мрежама података, тј. бежичном умреженом управљању и ваздушним *ad hoc* мрежама, најважнији фактор који ће **допринети сигурнијем небу** у будућности јесте **систематска свест** о постојећим **проблемима бежичног умрежавања**.

Чињеница је да је ваздухопловна индустрија, као једна од критичних националних инфраструктура, у претходној деценији, веома је брзо искористила напредак дигиталне технологије у циљу повећања ефикасности кључних процеса као што су системи за приказ информација о лету, ICT за управљање различитим операцијама у ваздухопловству, као и системи за руковање пртљагом на аеродромима. Интеграција алата ICT у механичке уређаји у рутинској употреби у ваздухопловној индустрији повећавају забринутост за сајбер безбедност. Обим инхерентних рањивости софтверских алата који покрећу ове системе ескалира, како се **ниво интеграције повећава**, а сектор ваздухопловства све више ″улази″ у сајбер простор, чинећи да **сајбер безбедност** постане **нови пејзаж за безбедност ваздухопловства**. Дакле, безбедносни изазови се повећавају како се убрзава еволуирање ваздухопловне индустрије, а ваздухопловна индустрија би требало да се прилагоди овом новом амбијенту, тј. да омогући ефикасно решавање сајбер-безбедносних изазова својствених огромној мрежи повезаних ваздухопловних технологија. Главни сајбер-безбедносни изазови у вези су са коришћењем ***e-Enabled*** авиона и ***smart*** (паметних) **аеродрома**; концепт ″паметни″ у индустрији цивилног ваздухопловства има корен у најсавременијим применама дигиталне индустрије, као што је интеграција уређаја са **IoT**, сензора у физичким системима, употреба вештачке интелигенције, као и велике количине података у ″облаку″, у циљу одржавања квалитета пружања услуга, тј. остваривања побољшаног корисничког искуства на поуздан и одржив начин, уз максималну оперативну ефикасност, безбедност и сигурност. Дакле, прелазак на све већи ниво аутоматизације кроз интеграцију оперативних система, формира нове површине за сајбер нападе, што резултира неопходношћу ревизије постојећих имплементација

сајбер-безбедности, процену последица нових претњи у развоју, као и ажурирање и анализу сценарија ризика и мере сајбер-безбедносне отпорности авио-сектора.

Оно што креира **широк спектар потенцијалних сајбер претњи** су природа система ваздухопловне индустрије, који су **хиперповезани** и **међузависни**, затим, **недостатак глобалних, консолидованих прописа**, као и **имплементација нових технологија с непознатим ризицима** – поред значаја сигурности, веома је важна сајбер безбедност, с обзиром на фреквентне сајбер нападе на овај критични инфраструктурни сектор. Сајбер безбедност је добила на нарочитом значају, трансформацијом традиционалних навигационих система (аналогни земаљаки системи) у дигиталне, свемирски засноване системе, у циљу прилагођавања огромном порасту густине ваздушног саобраћаја, тј. остваривања ефикаснијег и безбеднијег управљања ваздушним саобраћајем. Дакле, за прилагођавање традиционалних инфраструктурних система (укључујући системе за комуникацију, навигацију и надзор) очекиваном порасту авио-саобраћаја и решавање нових изазова, неопходно је ажурирање, тј. коришћење модерне технологије, која омогућава постизање већег капацитета, тачности и поузданости. У том циљу, критична инфраструктура система за ваздушну навигацију, трансформисана је из земаљских аналогних система у свемирске дигиталне системе. На пример, за комуникацију ваздух–земља између пилота и АТС, уместо аналогне VHF говорне комуникације, користе се приступи као што су контролор–пилот *data link* комуникација (CPDLC) и сателитска комуникација (SATCOM), које покривају широко географско подручје. Затим, коришћење GNSS система је прихватљивије у односу на земаљска навигациона средства, која имају бројна ограничења, као што су значајни трошкови инсталације и периодичне инспекције лета. Поред тога, уместо коришћења примарног и секундарног радара за надзор (PSR и SSR), могу се користити ADS–B и свемирски ADS–B, у зависности од сателитских система, чиме се постиже већа покривеност и тачност надзора, уз истовремено значајно смањење трошкова. Све ово трансформише и системе управљања ваздушним саобраћајем, из архитектуре засноване на размени података од једне тачке до друге, у архитектуру глобалне интероперабилности на нивоу целог система. Међутим, ваздухопловна индустрије суочава се с великим безбедносним ризицима у свим својим деловима, од система контроле летења, до авиона. На пример, навигациона средстава, поред тога што су подложна различитим рањивостима услед природних интерференција, као и људског фактора, имају и веома једноставан протокол отвореног дизајна, који има тенденцију занемаривања безбедносних проблема (не обезбеђује потпуну аутентификацију и енкрипцију). Због свега овога, **неопходно** је да **ваздухопловна индустрија ухвати корак** с **најновијим достигнућима** у вези са **безбедношћу бежичних комуникационих мрежа,** у циљу **одржавања високог нивоа сигурности и репутације** у **будућности**. При томе, у ваздухопловној индустрији, од пресудног значаја су **сајбер-безбедносни прописи**, а овај критични национални инфраструктурни сектор веома је свестан потребе за додатним финансијским улагањима, као и чињенице да се одређене активности предузимају само онда када то захтевају регулативе.

Као што је истакнуто, један од најзначајнијих корака у ваздухопловству, тј. у модернизацији АТС је прелазак на ADS–B, интегрални део *NextGen* (FAA) и CASCADE (Eurocontrol) програма за унапређење ваздушног саобраћаја и то у

погледу безбедности, економичности, аутоматизације, екологије, итд. Овај систем надзора, заснован на GPS-у (сателитски систем за навигацију), може функционисати као предајник (ADS–B Out), или пријемник (ADS–B In) – ваздухоплов аутоматски преноси (ADS–B Out) и/или прима (ADS–B In) идентификационе и податке о позицији у режиму емитовања преко *data link* сателитских система. ADS–B је дизајниран за побољшање кључних сегмената ваздушног саобраћаја – познати бенефити употребе ове технологије, осим што су веома корисни за АТС, веома су значајни и авио-компанијама, летачкој посади и путницима. ADS–B In функција представља додатне могућности за уштеду горива и времена, нарочито коришћењем „*In Trial Procedures*" за безбедне летове на великим удаљеностима у океанским ваздушним просторима, као и значајно повећава свест пилота о ситуацији омогућавајући приступ скоро истим подацима које су на раполагању земаљским АТС оператерима. Свакако, **ADS–B** ће **допринети компактности ваздушног простора, смањујући међупростор између авиона** на мање од 3 NM**,** као и омогућити **додатне функционалности** (извештаји о метеоролошким условима, земаљско мапирање, функционалност веома прецизног система за избегавање судара у ваздуху, решавање конфликтних ситуација**,** итд.). Међутим, ADS–B систем има и неколико веома важних недостатака, као што је зависност од сателитског навигационог система, тј. GPS/GNSS-а, који може бити физички оштећен, корумпиран или подложан сметњама. Такође, **ADS–B емитује информације преко отворених и нешифрованих протокола**, који користе једноставно кодирање грешака, тако да се може једноставно компромитовати коришћењем постојећих хардвера и софтвера, што представља кључне рањивости дизајна, тј. велики безбедносни ризик. Као што је претходно наглашено, ADS–B може бити изложен различитим врстама **сајбер напада**, као што су **прислушкивање**, **ометање** и **лажирање** (спуфинг): у нападу прислушкивања, нападач (само) прима бежични сигнал, у нападу ометања, нападач преноси бежични сигнал у циљу блокирања ADS–B сигнала, док код спуфинга, нападач може ињектирати, обрисати или изменити садржај ADS–B поруке (нападачи могу изменити ADS–B поруке и виртуелно модификовати путање лета авиона, креирати "авионе–духове" на екранима АТС, као и обрисати ADS–B поруке, што доводи до нестанка циљева са АТС екрана).

Предложене метеодологије за квалитативну и квантитативну процену сајбер-безбедносног ризика, омогућавају **систематизацију врсте напада** за постојећу, као и критичну инфраструктуру следеће генерације у ваздухопловним системима. Најскорије анализе показују да су **највиши ниво безбедносног ризика** имају гласовна **комуникација UHF**, **сателитска навигација** и **ADS–B**, а да су они с најнижим нивоом ризика контролор–пилот *data link* комуникација, земаљска радио-навигациона средства и секундарни радар. Свакако, константни напредак компактне и исплативе **SDR технологије снижава баријеру** за спровођење различитих **малициозних активности**, а узимајући у обзир обим и предстојећи степен имплементације ADS–B, неопходно је сагледати цео спектар сајбер-претњи на ADS–B, као и осмислити/предложити ефикасне стратегије ублажавања. Импликације, уколико ове стратегије изостану, могу довести до критичног угрожавања сектора цивилног ваздухопловства, од озбиљних финансијских губитака, до опасности од губитка људских живота.

Чињеница је да је **ваздухопловни систем сложен** и **динамичан систем** и налази се у константном стању промена, које се односе на усвајање нових технологија, процедура, процеса и система. Дакле, природа **ризика и опасности** су такође **динамичне** и **мењају** се током времена, односно непредвидиве су. Стога, средњорочно и дугорочно гледано, ова **константна еволуција ваздухопловног система**, **отвара бројна безбедносна питања**. При томе, сајбер претње користе сајбер преступници, тј. особе које имају непријатељске намере, знање из IT, као и приступ поверљивим информацијама (терористичке групе, њихови симпатизери, малициозни хакери и сл.) у циљу остваривања различитих оштећења авио система – нападима су изложени сви делови авио система, од система контроле летења, преко авиона и авио компанија, до аеродрома и пасошке, као и царинске контроле. У контексту унапређења комуникација коришћењем ваздухопловних мрежа, **увођење COTS** софтверских и хардверских решења, затим, **енормни пораст броја IoT** (IoT је фузија различитих технологија, тако да сви постојећи сајбер-безбедносни проблеми конвергирају ка IoT – у овој парадигми, управљање безбедношћу је огроман изазов), као и **BYOD** (различити уређаји, као што су *iPhones, iPads, Anroids* и *Tablets*), су и безбедносни ризик, с обзиром на то да се интегритет авио система, између осталог, може угрозити активном манипулацијом података (прислушкивањем, ометањем и спуфингом). Анализе различитих сценарија напада показују да одређени напади могу изазвати конфузију и представљати велики ризик због своје комлексности, као што су нпр. спуфинг напади (скоро сваки уређај који користи L1 цивилни GPS подложан је лажирању). Иако су ови **напади** на GNSS и **ADS–B** системе **потенцијална претња** – још увек су ретки потврђени извештаји о њиховој експлоатацији у цивилној авијацији, ризик по авио-сектор је веома висок, а изводљивост реална, услед брзог напретка јефтиних SDR платформи. Све ово нису једине промене парадигме која угрожава безбедност будућег ваздушног саобраћаја – веома важно питање је и **безбедна интеграција UAS/дронова** (који се могу користити и за спуфинг нападе из ваздуха у циљу отмице или дистракције безбедности у надзору ваздушног саобраћаја, на шта се мора обратити нарочита шажња, с обзиром на константни техничко/технолошки напредак), као и непредвиђени поремећаји (нпр. потенцијална претња примене квантног рачунарства за новоразвијене комуникационе протоколе засноване на криптографији). Стога, питања у вези са детекцијом и превенцијом спуфинга привлаче пажњу истраживача из области сајбер безбедности, а због могућих **софистициранијих спуфинг терористичких напада** на систем авиона, ICAO, RTCA и EUROCAE се проактивно баве побољшањем робусности GNSS и ADS–B у односу на RFI. Дакле, ваздухопловни сектор би требало да донесе адекватне закључке разматрањем садашњег сајбер-безбедносног стања и развије процесе који се брже прилагођавају његовим изазовима, како с техничког аспекта, тако и с аспекта људског фактора.

Сајбер преступници различитих профила већ су показали да могу угрозити функционисање читавог авио-система. Питање је да ли то могу остварити и терористи. Ипак, када се разматрају познати **сајбер инциденти**, сматра се да **немају опасан/критичан** утицај на **безбедност** авиона и путника. Међутим, с обзиром на ограниченост доступних извора у вези с пријављеним/реалним сајбер инцидентима у сектору цивилног ваздухопловства, највероватније постоје и сајбер

инциденти који нису јавно доступни. Ови непознати ризици, чине сагледавање утицаја различитих инцидентних ситуација на авио систем комплексним, а донекле га и доводе у питање. Ипак, систематизација и евалуација реалних сајбер инцидената, представљају полазну тачку и основу за предвиђања будућих трендова сајбер напада на авио-системе, као што је ADS–B, и дефинисања кључних категорија од значаја за разумевање сајбер сигурности/безбедности овог система као и развој и имплементације сајбер-противмера. При свему овоме, **само одговорно откривање новооткривене рањивости** је како од великог значаја за ваздухопловну индустрију, тако је и у националном интересу. Квантитативни резултати анализе ADS–B система показују да неки напади, као што је прислушкивање, имају релативно велику вероватноћу предузимања (због ниске цене ADS–B пријемника, недостатака безбедносних алгоритама и стандардизованих ADS–B протокола, итд.), али имају прихватљив/низак утицај на безбедност ваздухопловства. Међутим, ометање и лажирање, иако имају мању вероватноћу предузимања, у односу на прислушкивање, имају већи ризичан утицај на безбедност. У односу на поменуте врсте сајбер-напада, спуфинг напад (напад у којем се емитују лажни сигнали, који имитирају аутентичне сателитске сигнале, али веће снаге и различитог времена кашњења у односу на аутентичне сигнале, што доводи до тога да авион шаље нетачне информације о свом положају) има мању вероватноћу извођења, али највећи ниво безбедносног ризика. Предложене су многе **технике/методе** за **ублажавање напада** на **ADS–B**, засноване на коришћењу **криптографскских решења** или **верификацији локација**, док најскорије, развијају се технике засноване на **алгоритмима машинског учења**. За више информација о новим решењима за размену кључева и новим шифарским системима видети у научним радовима [586–588]. Свакако, академска истраживања у вези са сајбер безбедношћу не би требало да занемари знања и захтеве ваздухоловне заједнице, тј. специфичности овог сектора – фокусирање на изоловани проблем или технологије без разматрања целог система неизбежно доводи до непрактичних решења, тј. решења која неће имати примену.

Авио индустрија, као једна од критичних националних инфраструктура, поред значаја сигурности, захтева и веома висок ниво свих слојева безбедности, као и имплементацију високих индустријских безбедносних стандарда. Чињеница је да је међу свим облицима транспорта, ваздухопловна индустрија најнапреднија у **примени сајбер-безбедносних стандарда** – сектор ваздухопловства иде у корак с напредним ICT, веома их брзо усваја, и то углавном безбедно. Међутим, чињеница је и да су сајбер напади, који компромитују мету/е и доводе до политичких, као и економских контроверзи, у порасту. Краткорочно гледано, вероватноћа успешног сајбер напада на авио системи, па тако и ADS–B систем, предузета од стране појединца/недржавних актера веома је мала, услед тога што, с технолошког аспекта, авио-системи поседују методологију/алате и инструменте неопходне за решавање сајбер претњи. Међутим, интернет и рачунарске мреже веома су моћан ресурс, тако да постоји оправдана стрепња од успешног терористичког сајбер напада који може озбиљно угрозити функционисање нападнутог система с трагичним последицама. Такође, у наредним годинама, **сајбер криминалци/терористи** ће **усавршавати своје техничке вештине** захваљујући константно растућем црном тржишту малвера и других злонамерних софтвера, као

и развоја софистициринијих техничких уређаја. Ипак, како су истраживања показала, **доминантни интерес** сајбер криминалаца су **профитабилније** и **мање ризичне мете** као што су финансијски и комерцијални сектор цивилног ваздухопловства, а не нпр. АТС, и то не на начин који би довео до угрожавања људских живота. Свакако, превентивне и проактивне активности које се предузимају на националном нивоу за минимизирање ризика од сајбер напада, као и напори различитих међународних организација одговорних за постављање регулатива и смерница, које су у вези са сајбер безбедношћу (ICAO, EASA, итд.) минимизирају ризике од сајбер напада и додатна су препрека могућим сајбер нападима. Тако, од великог значаја јесте **развијање концепта сајбер безбедности** у ваздухопловству, дефинисаног од стране **ICAO** [23], као једне од водећих међународних организација одговорне за постављање регулатива и смерница који се односи на сајбер безбедност и отпорност сектора цивилне авијације, и то безбедност информационо-комуникационих система, технологија, као и њихове примене (аналогни и дигитални уређаји, радио станице, телекомуникације, компјутери, хардвер и софтвер, систем за складиштење података и уређаја, сателитске, навигационе и системе за надзор, као и различите с њима повезане услуге). Тако, прилагођена и најновије објављена ICAO стратегија, требало би да помогне у имплементацији ICAO визије о сајбер безбедности која кореспондира отпорности сектора цивилне авијације, без угрожавања иновативних техничко-технолошких решења. При томе, примена одговарајуће методологије за идентификацију потенцијалних претњи, анализа вероватноће ових претњи и њиховог утицаја на безбедност система цивилног ваздухопловства и екосистеме, омогућава процену нивоа ризика (квалитативну и квантитативну) као и њихово минимизирање/свођење на прихватљиви ниво кроз примену одговарајућих мера за ублажавање и контролу. Шта више, развијање пројеката као што је нпр. процена **утицаја сајбер безбедносних претњи** на **летачке операције** од стране **EASA**, фокусирана на неколико кључних авио-система, даје препоруке за ублажавање и спречавање могућих инцидентних ситуација. Најскорије (март, 2023) EASA је издала *Safety Information Bulletin* [589] информишући о интензивирању ометање (*jamming*) и/или лажирања (*spoofing*) GPS и ADS–B система у последњим месецима и дајући одређене препоруке заинтересованим странама, а који су, и према личном искуству, веома корисне пилотима, као крајњим корисницима ових авио-система. Ово је само један од начина на који EASA (као и друге организације на међународном нивоу), остварује свој примарни циљ – **одржавање високог, уједначеног нивоа безбедности цивилног ваздухопловства** у Европи, и нарочито ***cyber-awareness*** правовременог откривања и идентификације сајбер напада на сектор цивилне авијације.

Добити одговор на, чини се, једноставно питање, а то је **да ли је ваздухопловни систем безбедан** и сигуран у вези са сајбер претњама, веома је **комплексно** у својој анализи. Специфичне особине сајбер простора доводе нас до неспорне чињенице да је систем потпуно безбедан само уколико је искључен или уколико није у функције, и под условом да хакер претходно није успео да ″продре″ у систем, искористивши неку од рањивости система. Ипак, ова идеја о немогућности потпуне безбедности и сигурности система, не подразумева да различити нивои сајбер заштите не постоје, или да се не могу развити.

Цивилно ваздухопловство је **глобално најсигурнији облик транспорта** и систем у коме су ICT повезане у вероватно највећем обиму, у односу на друге системе засноване на ICT. Интеграција алата ICT у механичке уређаје у рутинској употреби у ваздухопловној индустрији повећала је забринутост у вези са сајбер безбедношћу, а обим инхерентних рањивости софтверских алата на којима се ови системи базирају, ескалира с повећањем нивоа интеграције. Штавише, ова забринутост постаје још акутнија с убрзавањем трансформације унутар ваздухопловне индустрије у вези с коришћењем ***e-Enabled* авиона** и **паметних аеродрома**. Тако, расте и број сајбер рањивости које могу бити експлоатисане од стране малициозне хакерске заједнице с различитим циљевима. Иако су ниво и учесталост сајбер напада на авио-системе, па тако и ADS–B, променљиви, оно што се највероватније неће мењати су намере нападача/малициозног хакера – угрожавање сигурности и безбедности различитих сегмената ваздухопловног авио система. Поред тога, очекује се континуирани пораст броја IT стручњака, при чему је у контекту националне сајбер безбедности, од кључног значаја осигурати да они ни на који начин не буду инволвирани у екстремистичке групе и радикалне идеологије. Због свега овога, поред **интердисциплинарности**, веома је важан и **мултидисциплинарни приступ**, тако да је подстицање сарадње између ваздухопловне и индустрије ICT за детекцију, истраживање и ублажавање сајбер претњи, један од приоритета. Наиме, експерименталним истраживањем требало би утврдити изводљивост и последице сајбер напада на ADS–B систем, на основу чега би се могле инкорпорирати правовремено адекватне против-мере. Ово подразумева сврсисходан проактивни приступ, уместо пост-реакција на инциденте/несреће и издавање нових прописа/процедура, као што је уврежено у сектору ваздухопловства.

Такође, за адекватан одговор или одбрану од напада на ADS–B, неопходна је систематска анализа, заснована на академском и стручном знању, као и јавно доступним подацима. **Бенефити** које пружа **ADS–B** су познати; систем **нуди више оперативних могућности**, као што су **ADS–B In апликације**, **детекција конфликта**, и **активности тражења/спашавања**. Такође, усвајање ове технологије даје велику количину података, тако да **анализе засноване на ADS–B подацима**, унапређују **валидацију питања сигурности/безбедности** (процена и праћење унапређења сигурности/безбедности, детаљне **анализе ризика**/опасности претходно идентификоване током истраге несреће/инцидента, **детектовање нових**/могућих **ризика** у динамичном окружењу и сл.). Ипак, како истиче ICAO, постоје одређене лимитације: дигитални ADS–B подаци илуструју – шта се догодило, али не дају директан и детаљан одговор на питање – зашто се инцидент догодио. За **потпуно разумевање ризика** и **генерисање ефикасних безбедносних ублажавања**, неопходно су анализе засноване на коришћењу **ADS–B података у комбинацији с другим скуповима података**. Такође, велика количина ADS–B података о лету је на располагању истраживачима, што омогућава **развој нових метода моделирања базираних на овим подацима надзора**. Свакако, FAA, EUROCONTROL и други ANSPs имају/чувају најсвеобухватније и најквалитетније податке о надзору ваздушног саобраћаја за одређени регион; међутим, све је једноставније добити ове податке путем јавних и комерцијалних извора (нпр. FlightAware, Flightradar24, OpenSky Network). Тако, из **података ADS–B** могу се

добити **квантитативне информације** које су инхерентно повезане са динамиком авиона и стога се и могу користити за поређење са предвиђањима динамичког модела. Односно, ADS–B омогућава фино подешавање параметара који омогућава праћење секвенце путање авиона, а која одговара одређеним фазама лета. Други примери ових истраживања обухватају моделирање потрошње горива, предвиђања перформанси, процене атмосферске емисије гасова у зависности од врсте авиона/региона, итд. При свему овоме, у циљу **спречавања погрешне примене ADS–B података** или злоупотребе, што би значајно деградирало успостављене и постигнуте напредке у безбедносним системима и програмима, покренуте су активности за **управљање процесом коришћења ADS–B информација** и биће развијене смернице за заштиту и примену најбоље праксе [590].

На крају, за разумевање сајбер напада на сектор цивилног ваздухопловства, па тако и на ADS–B, као веома важно истичемо **постојање свесности ситуације** – за неопходно повећање безбедности, сигурности и приватности ваздухопловног система, кључни фактор је свест о питањима сајбер безбедности у сектору авијације. Само повећање свесности ситуације, може довести до неопходних истраживања и развоја, и тако омогућити одговорним органима/организацијама да се баве проблемима, као и спречити експлоатације постојећих рањивости у будућности. Поред тога, **с аспекта људског фактора**, веома је значајна и **припрема за адекватну реакцију** пилота/контролора летења уколико дође до сајбер напада. Иако су нова ICT решења повећала безбедност информација и мрежа, као и омогућила детекцију претњи, недвосмислено је да је људска одлука, заснована на претходним знањима, искуствима и способностима, неопходна за успешно решавање критичних ситуација.

Јасно је да су бројне теме и питања које би требало анализирати у контексту међусобних релација цивилног ваздухопловства и сајбер безбедности, јер су и бројни елементи рањивости ваздухопловног система (нпр. интерни аеродромски компјутерски системи и *on-board* авио системи), и наричито хиперповезаност авио-система. Поред **техничког аспекта**, за комплетирање слике о сајбер нападима на сектор цивилне авијације, значајан аспект јесте **сагледавање вештина** и **потенцијала нападача**/актера (недржавних, државних и парадржавних) који представљају претњу за одређени авио систем. Свакако, сајбер-ризици у сектору цивилне авијације не могу се у потпуности елиминисати, али се могу ублажити/минимизирати **имплементацијом** веома **високих индустријских стандарда**, **адекватним безбедносним мерама**, **добром праксом** и **едукацијом**, како запослених, тако и корисника. При томе, **борба против сајбер претњи** је **заједничка одговорност** у којој **јавни, приватни** и **непрофитни сектор**, као и **појединци** и **сваки ниво власти**, имају своје **веома важне улоге** и **одговорности**. Стога, при идентификацији и реакцији на аномалну активност, сектор цивилне авијације може искористити своје, постојеће партнерске односе с локалним, националним и савезним агенцијама за спровођење законских регулатива као помоћ у предузимању адекватног одговора и налажењу решења.

ЛИТЕРАТУРА

1. Siu M., Goh D., Lim C. (2014) Aviation cyber security: a new security landscape. Journal of Aviation Management, 73–80. https://docplayer.net/2643432-Aviation-cyber-security-a-new-security-landscape.html (24/01/2023).
2. Kožović D., Đurđević D. (2019) Sajber bezbednost u avijaciji. Megatrend revija, 16(2), 39–56. doi:10.5937/MegRev1902039K.
3. Kožović D. (2019) Uloga i značaj sajber bezbednosti u vazduhoplovstvu. Master rad, Fakultet za civilno vazduhoplovstvo, Megatrend univerzitet, Beograd.
4. SenseCy (2016) Cyber Threats to the Aviation Industry – 2014, Netanya, Israel, 1–17. http://www.export.gov.il/files/hls/cyberthreatstotheaviationindustry.pdf?redire (23/02/2023).
5. Aviation Cyber Security Strategy – Moving Britain Ahead (2018) The Department for Transport, London, UK, 1–32. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/917529/aviation-cyber-security-strategy-document.pdf (26/02/2023).
6. Jeyakodi D. (2015) Cyber Security in Civil Aviation, For EALA Prize 2015, 1–19. https://manage.apricot.ie/uploads/upload/docs/1089/4._Deepika_Jeyakodi_Cyber_Security_in_Aviation.pdf (25/01/2023).
7. FAA (2020) NextGen Annual Report: a Report on the History, Current Status, and Future of National Airspace System Modernization. U.S. Department of Transportation, FAA, 155 p. https://www.faa.gov/sites/faa.gov/files/2022-06/NextGenAnnualReport-FiscalYear2020.pdf (01/03/2023).
8. SESAR (2020) European ATM Master Plan – Digitating Europe's Aviation Infrastructure, Executive view. 2020 edition, SESAR Joint undertaking, 176 p. https://www.sesarju.eu/sites/default/files/documents/reports/European%20ATM%20Master%20Plan%202020.pdf (01/03/2023). (01/03/2023).
9. Olaganathan R. (2018) Safety analysis of automatic dependent surveillance – broadcast (ADS-B) system, Int. J. Aerosp. Eng., 5(2), 9–18. https://commons.erau.edu/cgi/viewcontent.cgi?article=2107&context=publication (10/01/2023).
10. Ali B.S. (2016) System specifications for developing an automatic dependent surveillance-broadcast (ADS-B) monitoring system. Int. J. Crit. Infrastruct. Prot., 15, 40–46. doi:10.1016/j.ijcip.2016.06.004.
11. ICAO (2021) ADS-B Implementation and Operations Guidance Document, 14.0 ed., ICAO Asia and Pacific office, 2021, 144 p. https://www.icao.int/APAC/Documents/edocs/Revised%20ADS-B%20Implementation%20and%20Operations%20Guidance%20Document%20(AIGD)%20Edition%2014.pdf (15/03/2023).
12. Costin A., Francillon A. (2012) Ghost in the Air (Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices, Black Hat USA, 1–12. https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf (01/03/2023).
13. Manesh M.R., Kaabouch N. (2017) Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ads-b) system. Int. J. Crit. Infrastruct. Prot., 19(C), 16–31. doi:10.1016/j.ijcip.2017.10.002.

14. Kožović D., Đurđević D. (2021) Spoofing in aviation: security threats on GPS and ADS–B systems. Vojnotehnički glasnik/Mil. Tech. Cour., 69(2),461–485. doi:10.5937/vojtehg69-30119.
15. Kožović D., Đurđević D. (2021) Spufing u civilnoj avijaciji: bezbednost i sigurnost GPS/GNSS i ADS-B Sistema. Megatrend revija, 18(3), 281–306. doi:10.5937/MegRev2103281K.
16. Au M.H., You S.M., Li.J., Luo X., Wang C., Castiglione A., Kluczniak K. (eds.) (2018) Proceedings of the Network and System Security: 12th International Conference, NSS 2018, Hong Kong, China. doi:10.1007/978-3-030-02744-5.
17. Yang H., Zhou Q., Yao M., Lu R., Li H., Zhang X. (2019) A practical and compatible cryptographic solution to ADS-B security. IEEE Internet Things J., 6(2), 3322–3334. doi:10.1109/JIOT.2018.2882633.
18. Wang J., Zou Y., Ding J. (2020) ADS-B spoofing attack detection method based on LSTM. Eurasip J. Wirel. Commun. Netw.,160, 12p. doi:10.1186/s13638-020-01756-8.
19. Ying X., Mazer J., Bernieri G., Conti M., Buschell L., Poovendran R. (2019) Detecting ADS-B spoofing attacks using deep neural networks. Proceeding of the IEEE Conference on Communications and Network Security (CNS2019), Washington D.C., USA, 9 p. doi:10.1109/CNS.2019.8802732.
20. Hegarty C., Shallberg K., Walter T., Alexander K. (2018) Spoofing detection for airborne GNSS equipment Proceedings of 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, USA, 1350–1368.
21. Quadros F.D.A., Snellen M., Sun J., Dedoussi I.C. (2022) Global Civil Aviation Emissions Estimates for 2017–2020 Using ADS-B Data. J, Aircr., 59(6), 1394–1405. doi:10.2514/1.C036763
22. Kožović V.D., Đurđević Ž.D., Dinulović R.M., Milić S., Rašuo P.B. (2023) Air traffic modernization and control: ADS–B system implementation update 2022 – a review. FME Trans., 51(1), 117–130. doi: 10.5937/fme2301117K. https://www.mas.bg.ac.rs/_media/istrazivanje/fme/vol51/1/13_kozovic_at_al.pdf (15/03/2023).
23. ICAO, Aviation cybersecurity. https://www.icao.int/aviationcybersecurity/Pages/default.aspx (21/02/2023).
24. Toader E., Firtescu B.N., Roman A., Anton S.G. (2018). Impact of information and communication technology infrastructure on economic growth: an empirical assessment for the EU countries. Sustainability, 10(10), 3750, 22p. doi:10.3390/su10103750.
25. Pradhan, R.P., Mallik, G., Bagchi, T.P. (2018). Information communication technology (ICT) infrastructure and economic growth: A causality evinced by cross-country panel data. IIMB Manag. Rev., 30, 91–103. doi:10.1016/j.iimb.2018.01.001.
26. Mladenović, D.D. (2016) Multidisciplinarni aspekti sajber ratovanja, Doktorska disertacija, Univerzitet u Beogradu – Fakultet organizacionih nauka, Beograd.
27. Europeyou, What is information and communication technology. https://europeyou.eu/es/what-is-information-and-communication-technology/ (21/02/2023).
28. Maurer T., Morgus R. (2014) Compilation of Existing Cybersecurity and Information Security and Related Definitions, Report, Federal Department of Foreign Affairs, Switzerland.

https://d1y8sb8igg2f8e.cloudfront.net/documents/compilation-of-existing-cybersecurity-and information-security-related-definitions.pdf (01/02/2023).
29. Yamin M. (2019) Information technologies of 21st century and their impact on the society. Int. J. Inf. Technol., 11(4), 759–766. doi:10.1007/s41870-019-00355-1.
30. West D., Heath D. (2011) Theoretical pathways to the future: globalization, ICT and social work theory and practice. J. Soc. Work, 11(2), 209–221. doi:10.1177/1468017310386835.
31. Sorj B. (2008) Information societies and digital divides – an introduction. Polimetrica, Milano, Italy. https://www.researchgate.net/publication/220487000_Information_Societies_and_Digital_Divides (15/02/2023).
32. Webster F. (2006) Theories of the Information Society. 3rd ed., Routledge. Abingdon, UK. http://www.kultx.cz/wp-content/uploads/theories-of-the-information-society-by-frank-webster.pdf (21/02/2023).
33. Vuletić D. (2015) Smernice za izradu strategije obezbeđenja sajber prostora. Vojno delo, 67(5), 167–180. doi: 10.5937/vojdelo1505167V
34. Luknar I. (2019) Borba protiv kiberterorizma u strateškim dokumentima Republike Srbije, Doktorska disertacija, Univerzitet u Beogradu – Fakultet političkih nauka, Beograd.
35. Vakulyk O., Petrenko P., Kuzmenko I., Pochtovyi M., Orlovskyi R. (2020) Cybersecurity as a component of the national security of the state. J. Secur. Sustain. Issues, 9(3), 775–784. doi:10.9770/jssi.2020.9.3(4).
36. Kianpour M., Kowalski S.J. Øverby H. (2022) Advancing the concept of cybersecurity as a public good. Simulat. Model. Pract. Theor., 116, 102493–102509. doi:10.1016/j.simpat.2022.102493.
37. Leiner M.B., Cerf G.V., Clark D.D., Kahn E.R., Kleinrock L., Lynch D.C., Postel J., Roberts G.L., Wolff S. Brief History of the Internet 1997. Internet Society. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (21/ 02/2023).
38. Scaparrotti M.C. (2014). USA – Department of Army, Information Operations, Joint Publication, 3–13. https://irp.fas.org/doddir/dod/jp3_13.pdf (15/02/2023).
39. Strategija za borbu protiv visokotehnološkog kriminala za period 2019–2023. godine. (2018) "Sl. glasnik RS" br. 71/2018-49. http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg (23/02/2023).
40. Dempsey E.M. (2013) Defending the Nation at Network Speed. A discussion on cybersecurity
with general Martin E. Dempsey, U.S. Army. DEFENSE, Brookings Institution, 2013, Washington, D.C., USA. https://www.brookings.edu/wp-content/uploads/2013/06/20130627_dempsey_cybersecurity_transcript.pdf (21/02/2023).
41. Vuletić D. (2017). Upotreba sajber prostora u kontekstu hibridnog ratovanja, Vojno delo, 69(7), 308–325. doi: 10.5937/vojdelo1707308V
42. Libicki C.M. (2010) Cyberdeterrence and cyberwar, Rand project air force, 1–214 https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (15/02/2023).
43. Richardson C.J. (2012) Bridging the Air Gap: An Information Assurance Perspective. Engineering Doctorate, University of Southampton, Electronics and Computer Scienc. Defence College of Communications and Information Systems.

https://eprints.soton.ac.uk/355926/1/Richardson.pdf (20/02/2023).
44. TRADOC Pamphlet 525-7-8 (2010) The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028. https://www.acqnotes.com/Attachments/Cyberspace%20Operations%20Concept%20Capability%20Plan%202016-2028.pdf (21/02/2023).
45. Acqnotes, Information techology – cyberspace. https://acqnotes.com/acqnote/careerfields/cyberspace (11/02/2023).
46. Pallab Ghich, BBC News (2023) Quantum breakthrough could revolutionise computing. https://www.bbc.com/news/science-environment-64492456 (16/03/2023).
47. Stevanović D. M., Đurđević D. (2016) Internet stvari, lična i materijalna bezbednost. Bezbednost, 58(3), 113–128. https://scindeks-clanci.ceon.rs/data/pdf/0409-2953/2016/0409-29531603113S.pdf (15/03/2023).
48. McGraw G. (2013) Cyber war is inevitable (unless we build security in). J. Strateg. Stud., 36(1), 109–119. doi:10.1080/01402390.2012.742013.
49. Mladenović D., Jovanović D., Drakulić M. (2012) Definisanje sajber ratovanja. Vojnotehnički glasnik/Mil. Tech. Cour., 60(2), 84–117. doi:10.2298/vojtehg1202084M.
50. Libicki M. (2014) Why Cyber War Will Not and Should Not Have Its Grand Strategist. Strategic Studies Quarterly (SSQ), 8(1), 23–39. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-08_Issue-1/Spring_2014.pdf (14/02/ 2023).
51. Clarke R., Knake R. (2010) Cyber War: The Next Threat to National Security And What To Do About It, Harper-Collins e-books. https://indianstrategicknowledgeonline.com/web/Cyber%20War%20-%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20%28Richard%20A%20Clarke%29%20%282010%29.pdf (11/03/ 2023).
52. Stevanović D.M., Đurđević D. (2020) Uloga i značaj računarske forenzike u suzbijanju terorizma. Megatrend revija, 17(1) 129–142. doi:10.5937/MegRev2001129S.
53. Steve Ranger (2020) What is the IoT? Everything you need to know about the Internet of Things right now. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (17/02/2023).
54. Patel K.K., Patel S.M. (2016) Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput., 6(5), 6122–6131. doi:10.4010/2016.1482
55. Jacob Cass (2023) Internet of Things: What It Is, How It Works, Examples and More. https://justcreative.com/internet-of-things-explained/ (20/02/2023).
56. Pier Paolo Ippolito (2019) An Introduction to the Internet of Things. https://www.freecodecamp.org/news/introduction-to-iot-internet-of-things/ (21/02/2023).
57. Samoobrazovanje (2019) Šta je Internet of Things (Internet inteligentnih uređaja). https://samoobrazovanje.rs/sta-je-internet-of-things-internet-inteligentnih-uredjaja/ (21/02/2023).
58. John Terra (2022) Top 35 IoT Terms You Need to Know. https://www.simplilearn.com/top-iot-terms-you-need-to-know-article/ (21/02/2023).

59. Bellekens X., Seeam A., Nieradzinska K., Tachtatzis C., Cleary A., Atkinson R., Andonovic I. (2016) Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures. https://doi.org/10.6084/m9.figshare.3971523.v1. (01/02/2023).
60. Mijalković S. (2011) Obaveštajno-bezbednosne službe i nacionalna bezbednost. Bezbednost, 53(1), 74–92. https://scindeks.ceon.rs/article.aspx?artid=0409-29531101074M (05/02/2023).
61. Starr S. (2009) Toward a preliminary theory of cyberpower. In Kramer D. F., Starr H.S., Wentz L. (eds.): Cyberpower and national security, Washington, D.C. Potomac Books, USA, 43–88.
62. Gomez M.A. (2017) Victory in cyberspace. IAFOR J. Polit. Econ. Law, 4(1), 40–51. doi.org/10.22492/ijpel.4.1.04.
63. Vuletić D. (2017) Sajber bezbednost, u Integralna bezbednost Republike Srbije, ed. Forca B., Univerzitet „Union–Nikola Tesla", Beograd, Srbija, 169–184.
64. Mladenović D. (2012) Međunarodni aspekt sajber ratovanja. Medija centar Odbrana, Beograd, Srbija.
65. Lachow I. (2009) Cyber Terrorism: Menace or Myth?. In Kramer D. F., Starr H. S,. Wentz L. (eds.): Cyberpower and National Security, Washington D.C. Potomac Books, 437–464.
66. Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J. (2012) The law of cyber-attack. Cal. L. Rev., 100(4), 822–832. https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack (02/02/2023).
67. Hansen, L., Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. Int. Stud. Q., 53(4), 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x.
68. ISO/IEC 25010:2011, Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models. https://www.iso.org/standard/35733.html (22/02/2023).
69. Shannon G. (2016) in David Talbot ″Why We're So Vulnerable″. MIT Technology Review. https://www.technologyreview.com/2016/01/25/163739/why-were-so-vulnerable/ (12/02/2023).
70. ATIS Telecom Glossary, s.v.″bug″. http://www.atis.org/glossary/definition.aspx?id=5964 (24/02/2023).
71. ATIS Telecom Glossary, s.v. "flaw". http://www.atis.org/glossary/definition.aspx?id=8016 (24/03/2023).
72. ATIS 3GPP Specification. https://www.atis.org/wp-content/uploads/3gpp-documents/Rel99-14/ATIS.3GPP.32.442.901-2010.pdf (15/03/2023).
73. ISO/CD 10303-226 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication939.pdf (15/03/2023).
74. Nick Lewis, NSA TAO: What Tailored Access Operations unit means for enterprises. https://www.techtarget.com/searchsecurity/tip/NSA-TAO-What-Tailored-Access-Operations-unit-means-for-enterprises (12/02/2023).
75. Kaspersky, What is a Zero-day Attack? - Definition and Explanation. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit (22/02/2023).
76. Joyce R. (2016) Disrupting Nation State Hackers (presented at USENIX Enigma 2016).

https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce (15/03/2023).
77. Smeets M. (2022) Cyber arms transfer: meaning, limits, and implications. Security studies, 31(1), 65–91. doi:10.1080/09636412.2022.2041081.
78. Neumann G.P. (2015) Illustrative Risks to the Public in the Use of Computer Systems and Related Technology. Computer Science Laboratory, SRI International, Menlo Park, CA, USA. http://www.csl.sri.com/users/neumann/illustrative.html#8 (22/02/2023).
79. Vuletić, D. (2012) Napadi na računarske sisteme. Vojnotehnički glasnik/Mil. Tech. Cour., 60(1), 235–249. doi:10.5937/vojtehg1201235V.
80. Arquilla J., Ronfeldt, D. (1993) Cyberwar is coming!. Comparative Strategy, 12(2), 141–165. doi:10.1080/01495939308402915. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (12/02/2023).
81. Zetter K. (2014) An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (21/02/2023).
82. Kushner D. (2013) The real story of stuxnet, IEEE Spectrum, 50(3). doi:10.1109/MSPEC.2013.6471059
83. Menn J. (2015) Exclusive: U.S. Tried Stuxnet-style Campaign against North Kora but Failed – Sources. Reuters. http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (22/02/2023).
84. Nakashima E., Warrick J. (2012) Stuxnet was Work of U.S. and Israeli Experts, Officials Say. The Washington Post. https://www.washingtonpost.com/world/nationalsecurity/stuxnet-was-work-of-us-and-israeli-experts-officialssay/2012/06/01/gJQAlnEy6U_story.html (21/02/2023).
85. Anderson N. (2012) Confirmed: US and Israel Created Stuxnet, Lost Control of it. Ars Technica, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lostcontrol-of-it/ (18/02/2023).
86. Iasiello E. (2013). Cyber attack: A dull tool to shape foreign policy. Proceedings of the 5th International Conference on Cyber Conflict (CYCON 2013), 451–468. Tallinn: NATO CCD COE. https://www.semanticscholar.org/paper/Cyber-attack%3A-A-dull-tool-to-shape-foreign-policy-Iasiello/fbb57a658b363c55a93c1e46d01b417c082fd9b6 (15/02/2023).
87. Lindsay J.R. (2013) Stuxnet and the limits of cyber warfare. Security Studies, 22(3), 365–404. doi:10.1080/09636412.2013.816122.
88. Allison A. (2013) Cyber "hostilities" and the war powers resolution. Mil. L. Rev., 217, 174–192. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2460068 (23/02/2023).
89. Tallinn Manual on the International Law Applicable to cyber warfare. (2013) Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, ed. Schmitt N. M. Cambridge University Press, UK, 140–141. https://assets.cambridge.org/97811070/24434/frontmatter/9781107024434_frontmatter.pdf (23/02/2023).
90. Buckland B.S., Schreier F., Winkler T.H. (2010) Demokratsko upravljanje: izazovi sajber bezbednosti, Forum za bezbednost i demokratiju, Beograd.
91. Nedeljković S., Forca B. (2015) Evropska strategija bezbednosti i saajber pretnje – značaj za Srbiju. Vojno delo, 67(3), 135–154. doi:10.5937/vojdelo 1503135N.

92. Kizza J.M. (2009). A Guide to Computer Network Security, Springer, London. doi:10.1007/978-1-84800-917-2.
93. Tirk Ž., García de Soto B., Mantha B.R.K., Maciel A., Georgescu A. (2022) A systemic framework for addressing cybersecurity in construction. Autom. Constr., 133, 103988–104002. doi:10.1016/j.autcon.2021.103988.
94. Craigen D., Diakun-Thibault N., Purse R. (2014) Defining cybersecurity. Technol. Innov. Manag. Rev., 4(10), 13–21. doi:10.22215/timreview/835.
95. Geer D., Jardine E., Leverett E. (2020) On market concentration and cybersecurity risk. J. Syber Policy, 5 (1), 9–29. doi: 10.1080/23738871.2020.1728355.
96. McLennan M. (2021) The Global Risks reports 2021. 16th Edition, World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (21/02/2023).
97. Baltezarević I., Baltezarević R. (2021) Sajber bezbednost: izgradnja digitalnog poverenja. Megatrend revija, 18(4), 269–280. doi:10.5937/MegRev2104269B.
98. von Solms R. (1998) Information security management (3): the code of practice for information security management (BS 7799). Inf. Manag. Comput. Secur., 6(5) 224–225. doi:10.1108/09685229810240158.
99. Paananen H., Lapke M., Siponen M. (2020) State of the art in information security policy development, Comput. Secur., 88(C), 101608–101638. doi:10.1016/j.cose.2019.101608.
100. von Solms R., van Niekerk J. (2013) Information security to cyber security. Comput. Secur., 38, 97–102. doi:10.1016/j.cose.2013.04.004.
101. ISO/IEC 27002:2005 (2005) Information technology –Security techniques – Code of practice for information security management. https://webstore.iec.ch/p-preview/info_isoiec27002%7Bed1.0%7Den.pdf (25/02/2023).
102. Whitman M.E., Mattord H.J. (2011) Principles of information security. 4rd ed. Thompson Course Technology, Boston, USA. http://almuhammadi.com/sultan/sec_books/Whitman.pdf (27/02/2023).
103. Mitnick K., Simon W. (2002) The art of deception: Controlling the human element of security. Wiley Publishing, New York, USA. https://repo.zenk-security.com/Magazine%20E-book/Kevin_Mitnick_-_The_Art_of_Deception.pdf (15/03/2023).
104. Wood C.C. (2004) Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Comput. Fraud Secur., 2004(1), 16–17. doi:10.1016/S1361-3723(04)00019-3.
105. AlHogail A., Mirza A. (2014) Information security culture: a definition and a literature review. IEEE World Congress on Computer Applications and Information Systems, Hammamet, Tunisia, doi:10.1109/WCCAIS.2014.6916579.
106. ISO/IEC 13335-1:2004 (2004) Information technology – Security techniques – Management of information and communications technology security – Part 1: concepts and models for information and communications technology security management. https://www.iso.org/standard/39066.htm (19/02/2023).
107. International Organization for Standardization, ISO/IEC Glossary of IT Security Terminology, ISO/IEC, https://www.iso.org/glossary.html (18/02/2023).
108. Совет Федерации Федерального Собрания Российской Федерации (2014) Концепция стратегии кибербезопасности Российской Федерации – Проект. 1–10. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (01/02/2023).

109. Pawlak P. (ed.) (2014) Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development (report) Institute for Security Studies, Paris. doi:10.2815/43313. https://www.files.ethz.ch/isn/186860/Report_21_Cyber.pdf (23/02/2023).
110. Centre for Cyber and Information Security at the Norwegian University of Science and Technology (NTNU CCIS), Cyber security versus information security. https://www.ntnu.edu/ccis/center-for-cyber-and-information-security (16/02/2023).
111. Abeyratne R. (2011) Cyber terrorism and aviation—national and international responses. J. Transp. Secur., 4(4), 337–349. doi:10.1007/s12198-011-0074-3.
112. Aviation is facing a rising wave of cyber-attacks in the wake of COVID. https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid (20/02/2023).
113. Matijašević Obradović J. (2014) The significance and modalities of internet abuse as the primary global communication computer networks in cyberspace, Megatrend revija, 11(1), 279–298. doi:10.5937/MegRev1401279M.
114. Saint-Claire S. (2011) Overview and analysis on cyber terrorism. https://web.p.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=19188722&AN=79345460&h=KmdoWVKdRK%2bxFyrWrbrn6KIRwcyx%2b1oReNjtmLyGGZV%2ff0nizvkX64BIGweUpUBZ%2bnt5nqJVrHKkOgSXUvfuew%3d%3d&crl=f&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d19188722%26AN%3d79345460 (15/02/2023).
115. SAP, What is IoT? https://www.sap.com/india/insights/what-is-iot-internet-of-things.html (20/02/2023).
116. Nadir I., Mahmood H., Asadullah G. (2022) A taxonomy of IoT firmware security and principal firmware analysis techniques. Int. J. Crit. Infrastruct. Prot., 38(C), 100552–100554. doi:10.1016/j.ijcip.2022.100552.
117. Alqahtani, S. H. (2016) Latest trends and future directions of cyber security information systems. *J. Inf. Eng. Appl.*, 6(11), 9–14. https://iiste.org/Journals/index.php/JIEA/article/view/34213 (20/02/2023).
118. Sommestad T. (2012) A framework and theory for cyber security assessments. Doctoral dissertation, Industrial Information and Control Systems KTH, Royal Institute of Technology Stockholm, Sweden. https://www.diva-portal.org/smash/get/diva2:561246/fulltext02 (15/02/2023).
119. Department of Homeland Security, Operational and Support Components. https://www.dhs.gov/operational-and-support-components (23/02/2022).
120. ICAO (2022) Annex 17 to the Convention on International Civil Aviation Security, Safeguarding International Civil Aviation a gainst Acts of Unlawful Interference, 12th ed. real. https://standart.aero/en/icao/book/annex-17-aviation-security-safeguarding-international-civil-aviation-against-acts-of-unlawful-interference-en-cons (15/03/2023)
121. ICAO (2007) Carriage of duty free liquids, gels and aerosols in cabin baggage – working toward a global response to immediate threats. https://www.icao.int/Meetings/AMC/MA/2007/9CCARDCA/9ccardcaip04.pdf (23/08/2022).

122. Daragahi Borzou (2010) Bin Laden takes responsibility for Christmas Day bombing attempt. Los Angeles Times. https://www.latimes.com/archives/la-xpm-2010-jan-24-la-fgw-bin-laden25-2010jan25-story.html (01/02/2022).
123. BBC News (2012) Underwear bomber Abdulmutallab sentenced to life. https://www.bbc.com/news/av/world-17069890 (23/02/2023).
124. McConnell D., Todd B. (2015) Al Qaeda Branch Calls for New Attacks Against the United States. CNN. https://edition.cnn.com/2015/08/04/middleeast/al-qaeda-branch-yemen-united-states/index.html (10/01/2023).
125. Cruickshank P., Robertson N., Shiffman K. (2012) How Safe is the Cargo on Passenger Flights. CNN. https://edition.cnn.com/2012/02/16/travel/cargo-terror-concerns/index.html (05/02/2022).
126. Robertson N., Cruickshank P., Lister T. (2011) Air cargo bomb threat Achilles heel of international aviation security. CNN. https://security.blogs.cnn.com/2011/09/08/air-cargo-bomb-threat-achilles-heel-of-international-aviation-security/ (14/11/2022).
127. Liscouski R., McGann W. (2016) The evolving challenges for explosive detection in the aviation sector and beyond, CTC Sentinel., 9(5), 1–6. https://ctc.westpoint.edu/wp-content/uploads/2016/05/CTC-SENTINEL_Vol9Iss515.pdf (12/5/2022) (13/02/2023).
128. ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity. https://www.iso.org/standard/44375.html (14/02/2023).
129. Klopfer F., Rizmal I., Sekuloski M., Hatzl T., Mladenović D. Uvod u upravljanje sajber bezbednošću – priručnik za narodne poslanike. https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyTool%20SERBIAN.pdf (15/02/2023).
130. Intelligents airports–your runnway to success. https://www.wipro.com/engineering-construction-operations/intelligent-airports---your-runway-to-success/ (15/03/2023).
131. Rife C.T., Tomlin C., Enge P. (2008) Scanning the issue: Special issue on aviation information systems. Proceedings of the IEEE, 96(12), 1898–1901. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4745655 (10/01/2023).
132. Shaikh F., Rahouti M., Ghani N., Xiong K., Bou-Harb E., Haque J. (2019) A review of recent advances and security challenges in emerging e-enabled aircraft systems,.IEEE Access, 7, 63164–63180. doi:10.1109/ACCESS.2019.2916617.
133. Compiled by Reuters bureau (2019) Factbox: What we know about Boeing 737 MAX crashes and what comes next. https://www.reuters.com/article/us-ethiopia-airplane-developments-factbo/factbox-what-we-know-about-boeing-737-max-crashes-and-what-comes-next-idUSKCN1RG1Q8 (12/12/2022).
134. Kumar S., Xu B. (2017) Vulnerability assessment for security in aviation cyber-physical systems. Proceedings IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 145– 150. doi: 10.1109/CSCloud.2017.17.
135. Olive M., Oishi R., Arentz S. (2006) Commercial aircraft information security – an overview of ARINC Report 811. Proceedings of the IEEE/AIAA 25th Digital Avionics Systems Conference (DASC), Portland, OR, USA, 12p. doi: 10.1109/DASC.2006.313761.
136. Lee I. (2020) Internet of things (IoT) cybersecurity: literature review and IoT cyber risk management. Future Internet, 12(9), 157, 21p. doi:10.3390/fi12090157.

137. Gopalakrishna K., Govindarasu, M., Jacobson D.W., Phares B.M. (2013) Syber security for aerports. J. Traffic Transp. Eng., *3(4)*, 365–376. doi:10.7708/IJTTE.2013.3(4).02.
138. McAfee Labs Threats Report (2018). https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-threats-report-dec-2018.pdf (24/01/2023).
139. Kessler C.G., Craiger J.P (2018) Aviation cybersecurity: an overview. National Training Aircraft Symposium (NTAS), 2018: The Changing Role of the Pilot**,** Embry-Riddle Aeronautical University. 37. https://commons.erau.edu/cgi/viewcontent.cgi?article=1191&context=ntas (01/02/2023).
140. EUROCONTROL History Book (2010) By John McInally, Head of Organisational Development 1991–2010. https://www.erocontrol.int/sites/default/files/2020-01/eurocontrol-history.pdf (05/12/2022).
141. EUROCONTROL Think Paper #12 - Aviation under attack from a wave of cybercrime. https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime) (01/02/2023).
142. Aviation is facing a rising wave of cyber-attacks in the wake of COVID. https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid (13/01/2023).
143. Simmons H.O. (2017) Cybersecurity in Aviation: Constant Vigilance Required. J. Air L. & Com., 82(4), 771–802. https://scholar.smu.edu/jalc/vol82/iss4/5 (20/11/2022).
144. ICAO (2013) Doc. 9885AN/492: Restricted, Air Traffic Management Security Manual, 1st Edition–ICAO, Montréal, QC, Canada, 2013. http://www.icscc.org.cn/upload/file/20190102/Doc.9985-EN%20Air%20Traffic%20Management%20Security%20Manual.pdf (05/09/2022).
145. O'Flaherty K. (2018) How to hack an aircraft. Forbes, Jersey City, New Jersey, USA. https://www.forbes.com/sites/kateoflahertyuk/2018/08/22/how-to-hack-an-aircraft/?sh=12a8a8a441d1 (14/02/2023).
146. De Zan T., d'Amore F., Di Camillo F. (2015) The Defence of Civilian Air Traffic Systems from Cyber Threats. Istituto Affari Internazionali (IAI) (with the support of Vitroci as well as of ENAV), IAI 15/23E, 1–67. https://www.iai.it/sites/default/files/iai1523e.pdf (10/11/2022).
147. Dave G., Choudhary G., Sihag V., You I., Choo K. K. R. (2022) Cyber security challenges in aviation communication, navigation, and surveillance. Comput. Secur., 112, 102516–102522. doi:10.1016/j.cose.2021.102516
148. ICAO (2016) Doc. 4444: PANS-Air Traffic Managed, 16th Edition, ICAO, 2016. https://ops.group/blog/2016-16th-edition-icao-doc-4444/ (14/02/2023).
149. Elmarady A.A., Rahouma K. (2021) Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. IEEE Access, 9, 143997–144016. doi:10.1109/ACCESS.2021.3121230
150. Lykou, G., Iakovakis, G., Gritzalis, D. (2019) Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. In Gritzalis D., Theocharidou M., Stergiopoulos G. (eds.): Critical infrastructure security and resilience. Advanced sciences and technologies for security applications. Springer, Cham. 245–260. doi:10.1007/978-3-030-00024-0_13.

151. Armencheva I., Atanasova N., Ivanov I. (2019) Cyber globalization as an in/stability factor. Int. J. Adv. Soc. Sci., V(13), 71–81. doi:10.18769/ijasos.531497.
152. McCarthy J., Mahoney W. (2012) SCADA threats in the modern airport, IJCWT, 3(4), 32–39. doi: 10.4018/ijcwt.2013100104.
153. Teso H. (2013) Aircraft Hacking HITB Security Conference Europe, Amsterdam, Netherlands. http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf (21/04/2022.).
154. Zetter K. (2015) Feds Say That Banned Researcher Commandeered a Plane. Wired. https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/ (03/06/2022).
155. GAO (2015) Information security, FAA Needs to Address Weaknesses in Air Traffic Control Systems, GAO-15-221, 1–39. https://www.gao.gov/assets/gao-15-221.pdf (10/11/2022).
156. ICAO (2011) The Twenty-First Meeting of the APANPIRG ATM/AIS/SAR Sub-Group (ATM/AIS/SAR/SG/21−IP/21) Bangkok, Thailand,.1–6. https://www.icao.int/APAC/Meetings/ATMAISSARSG21/IP21%20Status%20of%20NextGen.pdf (13/09/2022).
157. ICAO (2005) Annex 2 to the Convention on International Civil Aviation, Rules of the Air, 10th ed, ICAO, 2005. https://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf (01/09/2022).
158. Petrić S.M. (2016) Budućnost upravljanja vazdušnim saobraćajem: ATM master plan i SESAR. Tehnika–Menadžment, 71(3), 465–470. doi:10.5937/tehnika1603465P.
159. Williams J.H., Signore, T.L. (2011) National Airspace System Security Cyber Architecture, Case #10–4169-The MITRE Corporation, Approved for public release by the FAA, 1–6. https://www.mitre.org/sites/default/files/publications/10_4169.pdf (15/09/2022).
160. Pollard T., Clark J. (2019) Connected aircraft: cyber-safety risks, insider threat, and management approaches. Proceedings of the 52nd Hawaii International Conference on System Sciences, 3232–3240. doi:10.24251/HICSS.2019.390.
161. Akram R.N., Markantonakis K., Mayes K., Bonnefoi P.F., Sauveron D., Chaumette S. (2016) An efficient, secure and trusted channel protocol for avionics wireless networks. Proceedings of the IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 10p. doi:10.1109/DASC.2016.7777967.
162. Akram R.N., Markantonakis, K.M., Mayes K., Bonnefoi P.F., Sauveron D., Chaumette S. (2016) Security and performance comparison of different secure channel protocols for avionics wireless networks. Proceedings IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 1–8. doi:10.1109/DASC.2016.7777966.
163. ICAO (2007) Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Vol. III, 2nd ed., ICAO, Montreal, QC, Canada, 2007. http://www.spilve.lv/library/law/Annex%2010%20Volume%20III.pdf (12/11/2022).
164. ICAO (2017) Doc.10037: Global Operational Data Link (GOLD) Manual, 1th ed., ICAO, Montreal, QC, Canada, 2017. https://ops.group/dashboard/wp-

content/groupdocs/gen/Reference/ICAO-DOC10037-GOLD-First-Edition-2017-compressed.pdf (03/10/2022).
165. ARINC (2014) Datalink Ground System Standard and Interface Specification (DGSS/IS), Technical Standard 620–8. https://www.sae.org/standards/content/arinc620-8/ (21/11/2022).
166. Watkins B.C., Walter R. (2007) Transitioning from federated avionics architectures to integrated modular avionics. Proceedings of the *IEEE/AIAA 26th Digital Avionics Systems Conference* (DASC), Dallas, Texas, USA, 2.A.1-1–2.A.1-10. doi:10.1109/DASC.2007.4391842.
167. FAA. Controlled Flight Into Terrain. https://www.faa.gov/news/safety_briefing/2018/media/SE_Topic_18-11.pdf (02/12/2022).
168. Kochenderfer M.J., Holland J.E., Chryssanthacopoulos, J.P. (2012) Next-Generation airborne collision avoidance system, Linc. Lab. J., 19(1), 17–33. https://www.ll.mit.edu/sites/default/files/page/doc/2018-05/19_1_1_Kochenderfer.pdf (05/10/2022).
169. Berges M.P., Shivakumar A.B., Graziano T., Gerdes R., Celik B.Z. (2020) On the feasibility of exploiting traffic collision avoidance system vulnerabilities. arXiv:2006.14679. doi:10.48550/arXiv.2006.14679
170. https://www.redimec.com.ar/contenido/productos/thumb_800_600/1426865204.jpg (12/01/2023).
171. https://forums.x-plane.org/uploads/monthly_2021_06/7.jpg.852a3dfd00643fdfd5a8d1b0978b2497.jpg (12/01/2023).
172. https://forums.x-plane.org/uploads/monthly_2021_06/6.jpg.27866c58a762d7a06f421584c4edd530.jpg (12/01/2023).
173. Kochenderfer, M.J., Chryssanthacopoulos, J.P., Weibel, R.E. (2012) A new approach for designing safer collision avoidance systems. Air Traffic Control Q., 20(1), 27–45. doi:10.2514/atcq.20.1.27.
174. Smith, M., Moser D., Strohmeier M., Lenders V., Martinovic I. (2018) Undermining privacy in the aircraft communications addressing and reporting system (ACARS). Proc. Priv. Enh. Technol., 3, 105–122. doi:10.1515/popets-2018-0023.
175. Johnston M. (2018) The airplane transponder. https://calaero.edu/the-airplane-transponder/ (11/11/2022).
176. Skybrary. Transponder. https://www.skybrary.aero/index.php/Transponder (14/12/2022).
177. Ali B.S., Ochieng W., Schuster W., Majumder A., Chiew T. (2015) A safety assessment framework for the automatic dependent surveillance broadcast (ADS-B) system. Saf. Sci., 78, 91–100. doi:10.1016/j.ssci.2015.04.011.
178. Pavić A., Lalić B., Đurđević M. (2014) Osnove ADS-B tehnologije i osmatranje područja Republike Srbije bez radarske pokrivenosti. Zbornik radova Infoteh–Jahorina, 13, 419–424. https://infoteh.etf.ues.rs.ba/zbornik/2014/radovi/KST-2/KST-2-4.pdf (04/10/2022).
179. Skybrary. Head Up Display. https://www.skybrary.aero/index.php/Head_Up_Display (20/10/2022).
180. Flying. How It Works: Head-Up Display. https://www.flyingmag.com/how-it-works-head-up-display/ (20/08/2022).

181. Flight Safety Fondation (2019) Special report: Head-up guidance system technology – a clear path to increasing flight safety. 1–28. https://flightsafety.org/wp-content/uploads/2016/09/hgs_nov09.pdf (24/01/2022).
182. Heads Up: HUDS Could Have Been A Factor In Many Aircraft Accidents (2010) Aero News Network. http://www.aero-news.net/index.cfm?do=main.textpost&id=5ac0e4c6-f612-4335-b995-0ac891c2ed0a (10/02/2023).
183. Ryan J.N. (2015) Airline head-up display systems: human factors considerations. Int. J. Econ. Manag. Sci., 4(5), 248, 12 p. doi:10.4172/2162-6359.1000248.
184. Azooptics. Head-up Displays (HUD) in Aviation and Their Quality Considerations. https://www.azooptics.com/Article.aspx?ArticleID=1917 (04/01/2023).
185. https://www.istockphoto.com/photos/boeing-737-cockpit (11/02/2023).
186. Godwin III B.J., Kulpin A., Rauscher K.F., Yaschenko V. (eds.) (2014) Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2. The EastWest Institute, New York , USA, 56. https://www.files.ethz.ch/isn/178418/terminology2.pdf (11/06/2022).
187. Bergen L.P. September 11 attacks. Britanicca. September 11 attacks - The September 11 commission and its findings | Britannica (09/02/2023).
188. GAO (2020) Aviation cybersecurity, FAA should fully implement key practices to strengthen its oversight of avionics risks, GAO-21-86. https://www.gao.gov/assets/gao-21-86.pdf (21/01/2023).
189. Sathaye H., Schepers D., Ranganathan A., Noubir G. (2019) Wireless attacks on aircraft Instrument Landing Systems. Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 357–372. https://www.usenix.org/system/files/sec19-sathaye.pdf (01/02/2023).
190. Bellamy III W. (2020) Researcher Demonstrates Satellite Eavesdropping on In-flight Passenger Internet at Black Hat 2020. Avionics International. https://www.aviationtoday.com/2020/08/10/researcher-demonstrates-satellite-eavesdropping-flight-passenger-internet-black-hat-2020/ (05/01/2023).
191. Bellamy III W. (2020) GAO Report Says Airlines Need New Cybersecurity Testing Policy for Avionics Systems. Avionics International. https://www.aviationtoday.com/2020/10/23/gao-report-says-airlines-need-new-cybersecurity-testing-policy-avionics-systems/ (06/01/2023).
192. Wolf M., Minzlaff, M., Moser, M. (2014) Information technology security threats to modern e-enabled aircraft: A cautionary note. J. Aerosp. Inf. Syst. 11, 447–457. doi:10.2514/1.I010156.
193. Mäurer N., Gräupl T., Schmitt C. (2019) Evaluation of the LDACS cybersecurity implementation. Proceedings of the IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, USA, 10p. doi:10.1109/DASC43569.2019.9081786.
194. Kaloudi N., Li J. (2020) The ai-based cyber threat landscape: A survey. ACM Comput. Surv. (CSUR) 53(1), 1–34. doi:10.1145/3372823.
195. Sarker I.H. (2022) AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. SN Comput. Sci., 3(2), 158, 20 p. doi:10.1007/s42979-022-01043-x.
196. GAO (2009) Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls. GAO-09-399, 1–97. https://www.gao.gov/assets/gao-09-399.pdf (11/11/2022).
197. AOPA, TSA airport access security requirements.

https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements (21/02/2023).
198. Lykou G., Anagnostopoulou A., Gritzalis D. (2019) Smart airport cybersecurity: threat mitigation and cyber resilience controls. Sensors, 19(1), 19. doi:10.3390/s19010019.
199. Koroniotis N., Moustafa N., Schiliro F., Gauravaram P., Janicke H.A. (2020) Holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access 8, 209802–209834. doi:10.1109/ACCESS.2020.3036728.
200. Bouyakoub S., Belkhir A., Bouyakoub F.M., Guebli W. (2017) Smart airport: an IoT-based airport management system. Proceedings of the ICFNDS '17: International Conference on Future Networks and Distributed Systems, Cambridge, UK, 45, 1–7. doi: 10.1145/3102304.3105572.
201. Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A. (2015) Guide to industrial control systems (ICS) security. Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce, Washington, D.C., USA, Special Pub. 800–82 Rev. 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (09/01/2023).
202. ENISA (2016) Securing Smart Airports. https://www.enisa.europa.eu/publications/securing-smart-airports (25/12/2022).
203. Infosecurity (2008) Cyber security lacking at airports. https://www.infosecurity-magazine.com/news/cyber-security-lacking-at-airports/ (25/11/2022).
204. Rosencrance L., Advanced persistant threat (APT). https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT (15/01/2023).
205. Garcia, A.B., Babiceanu R.F, Seker R. (2021) Artificial intelligence and machine learning approaches for aviation cybersecurity: an overview. *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, Dulles, VA, USA, 1–8. doi:10.1109/ICNS52807.2021.9441594.
206. Murphy R.J., Sukkarieh M., Haass J., Hriljac P. (2015) Aerport Cooperative Research Program, ACRP Report 140, Guidebook on Best Practices for Airport Cybersecurity, Transportation research board, Washington, D.C. USA. http://trbcybersecurity.erau.edu/resources/acrp_rpt_140.pdf (01/02/2023).
207. Ranasinghe D. (2014) Technology the Backbone of World's Best Airport. Tech Edge, A CNBC Special Report. https://www.cnbc.com/2014/03/28/technology-the-backbone-of-worlds-best-airport.html (04/02/2023).
208. Transportation Security Administration (2014) Security Technologies. https://www.tsa.gov/about-tsa/security-technologies (15/09/2022).
209. Roman A. (2009) The New Sustainable Airport Manual. Presented at Airports Going Green Conference 2009. https://www.academia.edu/9265898/The_New_Sustainable_Airport_Manual_Airports_Going_Green_Conference (11/09/2022).
210. Rainie L., Anderson J., Connolly J. (2014) Cyber Attacks Likely to Increase. Pew Research Center's Internet Project. https://eloncdn.blob.core.windows.net/eu3/sites/964/2019/07/Elon-Pew-Cyber-Attacks-2025.pdf (07/09/2022).
211. Hamilton T., Ochmanek D. (2020) Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments. RAND Corporation, Santa Monica, USA, 1–27. https://www.rand.org/pubs/research_reports/RR4407.html (05/01/2023).

212. Gilmour S. (2014) Policing Crime and Terrorism in Cyberspace: An Overview. European Review of Organised Crime 1(1), 143–159. https://scholar.google.co.uk/citations?view_op=view_citation&hl=en&user=nUmI60gAAAAJ&citation_for_view=nUmI60gAAAAJ:Tyk-4Ss8FVUC (26/02/2023).
213. Lewis J., McAfee Report (2018) Economic impact of cybercrime–no slowing down. 1–28. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (16/01/2023).
214. Kunesh A. (2021) Lufthansa flying its Boeing 747, Airbus A350 on select intra-Europe routes. https://thepointsguy.com/2017/02/lufthansa-a350-tour/ (20/01/2023).
215. Stouffer K., Zimmerman T., Tang Chee.Y., Cichonski J., Pease M., Shah N., Downard W. (2020) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Discrete-based Manufacturing System Use Case. National Institute of Standards and Technology, Internal Report NISTIR 8183A, 3, 60 p. doi:10.6028/NIST.IR.8183A-3.
216. Matthew P. Barrett (2018) US National Institute of Standards and Technology (NIST) (2018) Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (03/12/2022).
217. EUROCONTROL (2021) Aviation under attack from a wave of cybercrime. https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime (03/12/2022).
218. Kaiser L. (2012) Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy, U.S. Department of Homeland Security, 2013-2023. http://trbcybersecurity.erau.edu/files/Transportation-Standards-Plan.pdf (21/12/2022).
219. European Union & EUROCONTROL 2016 Single European Sky ATM Research (SESAR) – Addressing Airport Cyber-Security - Final Report https://www.sesarju.eu/sites/default/files/documents/news/Addressing_airport_cyber-security_Full_0.pdf
220. Bokan B., Santos J. (2021) Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures. Proceedings Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 1–6. doi:10.1109/SIEDS52267.2021.9483736.
221. AIAA (2013) The Connectivity Challenge: Protecting Critical Assets in a Networked World. A Framework for Aviation Cybersecurity World, An AIAA Decision Paper, AIAA, Reston, Virginia, USA. https://docplayer.net/1332697-The-connectivity-challenge-protecting-critical-assets-in-a-networked-world-a-framework-for-aviation-cybersecurity-an-aiaa-decision-paper.html (10/11/2022).
222. EUROCONTROL (2012) Manual for National Air Traffic Management Security Oversight, 1st ed., Brussels. https://www.eurocontrol.int/sites/default/files/2019-06/13_121_manual_for_national_atm_security_oversight_v2_0_signed.pdf (15/12/2022).
223. Hodgkinson D., Johnston R. (2018) Aviation Law and Drones - Unmanned Aircraft and the Future of Aviation, Routledge Taylor & Francis Group, London and New York. https://inaca.or.id/wp-content/uploads/2019/11/Aviation-Law-and-Drones_-Unmanned-Aircraft-and-the-Future-of-Aviation.pdf (16/01/2023).

224. Dinulović, M. Rašuo, B., Slavković, N., Karić, Đ. (2022) Analysis of aspect and taper ratio on aeroelastic stability of composite shells, FME Trans., 50(3), 732–744. doi: 10.5937/fme2204732D.
225. Dinulović M., Trninić M., Rašuo B., Kožović D. (2023) Methodology for aeroacoustic noise analysis of 3-Bladed H-Darrieus wind turbine. Therm. Sci., 27(1A) 61–69. doi: https://doi.org/10.2298/TSCI2301061D.
226. CORDIS (2020) Aerobits - world smallest ADS-B receivers to safely integrate drones into European airspace. https://cordis.europa.eu/project/id/791438 (11/11/2021).
227. Uavionix, ADS inert and alert for UAS revisited. https://uavionix.com/ads-b-inert-and-alert-for-uas-revisited/ (03/01/2023).
228. Morales-Ferre R., Richter P., Falletti E., Fuente A., Lohan E. S. (2020) A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft. IEEE Commun. Surv. Tutor., 22(1), 249–291 doi:10.1109/COMST.2019.2949178
229. Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA) (2018) Cybersecurity risks posed by unmanned aircraft systems, 1–6. file:///C:/Users/Administrator/Downloads/825402.pdf (16/02/2021).
230. ICAO (2006) Doc.7300/9: Convention on International Civil Aviation, 9th ed., ICAO, Montreal, QC, Canada, 2006. https://www.icao.int/publications/documents/7300_cons.pdf (12/12/2022).
231. Doss, R., Piramuthu S., Zhou W. (eds.) (2019) Future network systems and security. Proceedings of the 5th International Conference, FNSS 2019, Melbourne, VIC, Australia. https://dokumen.pub/qdownload/future-network-systems-and-security-5th-international-conference-fnss-2019-melbourne-vic-australia-november-2729-2019-proceedings-1st-ed-2019-978-3-030-34352-1-978-3-030-34353-8.html (14/11/2022).
232. Pyzynski M., Balcerzak T. (2021) Cybersecurity of the unmanned aircraft system (UAS). J. Intell. Robot. Syst., 102, 35, 12 p. doi:10.1007/s10846-021-01399-x.
233. Geoff M., Steuter E. Drone nation: the political economy of america's new way of war, Lexington Books, USA, 2016.
234. ICAO, 12th Air Navigation Conference. https:// www.icao.int/Meetings/anconf12/pages/default.aspx (09/01/2023).
235. ICAO (2016) Working paper Assembly – 30th session Addressing Cybersecurity in Civil Aviation, A39-WP/17 EX/5 Appendix, ICAO, Montreal, QC, Canada**,** *2016***.** https://www.icao.int/Meetings/a39/Documents/WP/wp_017_en.pdf (16/11/2022).
236. IATA, IATA's Industry Priorities. https://www.iata.org/en/about/priorities/ (01/12/2022).
237. ECAC. https://www.ecac-ceac.org/about-ecac (26/02/2023).
238. EUROCAE. https://www.eurocae.net/ (11/01/2023).
239. EUROCAE. https://www.skybrary.aero/articles/european-organisation-civil-aviation-equipment-eurocae (11/01/2023).
240. ENISA. https://dig.watch/actor/european-union-agency-network-and-information-security (11/01/2023).
241. FAA. https://skybrary.aero/articles/federal-aviation-administration-faa (11/01/2023).
242. Biernacki H.M. (2001) ICAO Assembly Resolution A33-1, adopted as a part of the Aviation Security Plan of Action.

https://www.icao.int/meetings/fal12/documents/biernacki.pdf (26/02/2023).
243. ICAO model UAS regulations. https://www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx (02/02/2023).
244. ICAO (2010) Doc. 9960: The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation ICAO, Beijing, China, 2010. https://www.icao.int/secretariat/legal/Administrative%20Packages/Beijing_Convention_EN.pdf#search=The%20Convention%20on%20the%20Suppression%20of%20Unlawful%20Acts%20Relating%20to%20International%20Civil%20Aviation (10/12/2022)
245. ICAO, Increased use of unmanned aircraft systems (UAS). https://www.icao.int/annual-report-2021/Pages/emerging-and-cross-cutting-aviation-issues-increased-use-of-unmanned-aircraft-systems-uas.aspx (11/03/2022).
246. Schjolberg S.J. (2014) The Third Pillar for Cyberspace. Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace, 9th Edition, 1–17. https://www.cybercrimelaw.net/documents/140615_Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf (11/10/2022).
247. U. S. Department of transportation office of inspector general (2019). https://www.oig.dot.gov/sites/default/files/Announcement%20Letter%20-%20FAA%20Aviation%20Cybersecurity%20Initiative%5E5-1-19.pdf (20/01/2023) (02/03/2023).
248. European Commission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brisel, 1–20. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (06/01/2023).
249. Cybersecurity (2021) https://www.eeas.europa.eu/eeas/cybersecurity_en (11/01/2023).
250. World Economic Forum (2022) New European Union cybersecurity proposal takes aim at cybercrime. https://www.weforum.org/agenda/2022/09/new-european-union-cybersecurity-proposal-takes-aim-at-cybercrimes/ (24/01/2023).
251. Strategija razvoja informacionog društva i informacione bezbednosti u Republici Srbiji za period od 2021. do 2026. godine. (2021) "Sl. glasnik RS" br. 86/2021-5. http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg (26/02/2023).
252. https://www.srbija.gov.rs/vest/570340 (26/02/2023).
253. https://thegfce.org/about-the-gfce/ (26/02/2023).
254. https://www.un.org/disarmament/open-ended-working-group/ (20/02/2023).
255. Pavićević M., Kljajić M. (2021) Complex interconnection of cyber space and climate change. Ecologica, 28(101), 125–133. doi:10.18485/ecologica.2021.28.101.19.
256. Wohlfeld M., Tanner F. (2021) Comprehensive security and new challenges: strengthening the OSCE. IAI PAPERS,1–23. https://www.iai.it/sites/default/files/iaip2123.pdf (01/02/2023).
257. United Nations Office for Project Services. https://www.un.org/ruleoflaw/un-and-the-rule-of-law/united-nations-office-for-project-services/ (26/02/2023).
258. The EACCC: coordinating Europe's crisis response. https://www.nm.eurocontrol.int/NM/eacc.html (01/02/2023).

259. Direktorat civilnog vazduhoplovstva Republike Srbije. (2016). Postupci u Republici Srbiji u vezi sa opasnim situacijama u vazduhoplovstvu, DCV-DIR-PR-901ACM, 02, 6. 06. 2022. https://www.cad.gov.rs/upload/opasnesituacije/Postupci%20u%20RS%20u%20vezi%20sa%20opasnim%20situacijama%20u%20vazduhoplovstvu.pdf (20/02/2023).
260. http://cad.gov.rs/lat/strana/21331/aktuelnosti (15/11/2022).
261. Zakon o vanrednim situacijama (2012) "Sl. glasnik RS" br. 111/2009, 92/2011 i 93/2012, član 8. https://www.paragraf.rs/propisi_download/zakon_o_vanrednim_situacijama.pdf (26/02/2023).
262. Zakon o smanjenju rizika od katastrofa i upravljanju vanrednim situacijama, "Sl. glasnik RS", br. 87/2018, https://www.paragraf.rs/propisi_download/zakon-o-smanjenju-rizika-od-katastrofa-i-upravljanju-vanrednim-situacijama.pdf) (26/02/2023).
263. Stastny P., Stoica A-M. (2022) Protecting aviation safety against cybersecurity threats. IOP Conf. Ser.: Mater. Sci. Eng., 1226, 012025. doi:10.1088/1757-899X/1226/1/012025.
264. FAA (2017) Safety management system components. https://www.faa.gov/about/initiatives/sms/explained/components/ (16/02/2023).
265. Stolzer A.J. (2017) Safety management systems in aviation. Taylor and Franci eBook, New York, USA. doi:10.4324/9781351149648.
266. ICAO (2020) Annex 17, Security — Safeguarding International Civil Aviation Against Acts of Unlawful Interference, 11th ed., ICAO, Montréal, Quebec, Canada, 2020. https://usermanual.wiki/m/fb9358c50374acc56f3940991956aef173c4ebd835cda9ac89d67cb9c9ff7a14.pdf (20/02/2023).
267. Andersen A.C. (2011) Comparative Analysis of Multilateration Methods for Signal Emitter Positioning. 1–9. http://files.andersen.im/analytics/Convex%20Optimization%20%20Comparative%20Analysis%20of%20Multilateration%20Methods%20for%20Signal%20Emitter%20Positioning.pdf (16/02/2023).
268. Strohmeier M., Schäfer M., Pinheiro R., Lenders V., Martinovic I. (2017) On perception and reality in wireless air traffic communication security. Trans. Intell. Transp. Syst., 18(6), 1338–1357. doi:10.1109/TITS.2016.2612584.
269. Baghdasarin D. (2019) MRO Cybersecurity SWOT. Int. J. Aviat. Aeronaut. Aerosp., 6(1), 1–5. https://doi.org/10.15394/ijaaa.2019.1318.
270. Jacobson D., Idziorek J. (2012) Computer Security Literacy: Staying Safe in a Digital World. 1st ed., Chapman & Hall/CRC Press, Boca Raton, USA.
271. Volpe J. A. (2001) Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Final Report. National Transportation Systems Center, 99 p. https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf (27/02/2023).
272. ICAO (2014) Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Vol. IV Surveillance Radar and Collision Avoidance Systems., 5th ed., ICAO, Montreal, QC, Canada, 2014. https://store.icao.int/en/annex-10-aeronautical-telecommunications-volume-iv-surveillance-radar-and-collision-avoidance-systems (27/02/2023).
273. Bauer F.H., Moreau M.C., Dahle-Melsaether M.E., Petrofski W.P., Stanton B.J., Thomason S., Harris G.A., Sena R.P., Parker Temple III L. (2006) The GPS space

service volume. Proceedings 19th I*nternational Technical Meeting of the Satellite Division of the Institute of Navigation (*ION GNSS+ 2006), Fort Worth, TX, USA, 2503–2514. https://www.ion.org/publications/abstract.cfm?articleID=6861 (27/02/2023).
274. Force D.A., Miller J.J. (2013) Combined global navigation satellite systems in the space service volume. Proceedings of the 2013 International Technical Meeting of the Institute of Navigation, San Diego, CA, USA, 803–807. https://core.ac.uk/download/pdf/42702928.pdf (27/02/2023).
275. Hein G.W. (2020) Status, perspectives and trends of satellite navigation. Satell. Navig., 1, 1–12, doi:10.1186/s43020-020- 00023-x.
276. Choi B.-K., Roh K.-M., Ge H., Ge M., Joo J.-M., Heo M.B. (2020) Performance analysis of the Korean Positioning System using observation simulation. Remote Sens. 12(20), 3365. doi:10.3390/rs12203365.
277. Ji G.-H., Kwon K.-H., Won J.-H. (2021) GNSS Signal Availability Analysis in SSV for Geostationary Satellites Utilizing Multi-GNSS with First Side Lobe Signal over the Korean Region. Remote Sens., 13(19), 3852. doi:10.3390/rs13193852.
278. NASA (2021) NASA Artemis Programme. https://www.nasa.gov/specials/artemis/ (27/02/2023).
279. ESA (2021) Who's Ready to Serve the Lunar Missions. https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Who_s_ready_to_serve_the_lunar_missions (27/02/2023).
280. SSTL (2021) Lunar Pathfinder Mission. https://www.sstl.co.uk/what-we-do/lunar-mission-services (27/02/2023).
281. URATS (2017) Communications, Navigation, and Surveillance (CNS) Technologies, IATA, URATS edition 3.0, 1–47. https://www.iata.org/contentassets/fb1df0e634454acc9207418a5d1d636b/requirements-urats-cns-technology_edition203_2017.pdf (20/02/2023).
282. Global Positioning System (GPS) Standard Positioning Service (SPS) Performance Analysis Report (2014) FAA GPS Product Team, Washington, USA, Report #86, 2014 https://www.nstb.tc.faa.gov/reports/PAN86_0714.pdf (27/02/2023).
283. ICAO (2018) Annex 10 to the Convention on International Civil Aviation, Aeronautical Telecommunications, Vol. I, Radio Navigation Aids, 7th ed., ICAO, Montreal, QC, Canada, 2018. https://www.iacm.gov.mz/app/uploads/2018/12/an_10_v1_Aeronautical-Telecommunications_7ed._2018_rev.91_01.07.18.pdf (27/02/2023).
284. ICAO (2017) Doc. 9849: Global Navigation Satellite System (GNSS) Manual, 3rd ed., ICAO, Montreal, QC, Canada, 2017. https://store.icao.int/en/global-navigation-satellite-system-gnss-manual-doc-9849
285. Samama N. (ed.) (2007) Development, deployment, and current status of satellite-based navigation systems. In Global positioning – Technologies and Performance, John Wiley& Sons, New Jersey, USA, Chapter 3, 57–93. doi:10.1002/9780470241912.ch3.
286. Global Positioning System Standard Positioning Service Signal Specification (1995) GPS SPS Signal Specification, 2nd ed. https://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf (27/02/2023).
287. Gaspar J., Ferreira, R., Sebastião P., Souto N. (2020) Capture of UAVs Through GPS Spoofng Using Low-Cost SDR Platforms. Wirel. Pers. Commun., 115(4), 2729–2754. doi:10.1007/s11277-020-07211-7.

288. Schmidt D., Radke K., Camtepe S., Foo E, Ren M. (2016) A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Comput. Surv., 48(4), 1–31, doi:10.1145/2897166.
289. Li X., Zhang X., Ren X., Fritsche M., Wickert J., Schuh H. (2015) Precise positioning with current multi-constellation Global Navigation Satellite Systems: GPS, GLONASS, Galileo and BeiDou. Sci. Rep., 5, 8328. doi:10.1038/srep08328.
290. Verhagen S. Teunissen P. J. G. (2014) Ambiguity resolution performance with GPS and BeiDou for LEO formation flying. Adv. Space Res., 54(5), 830–839. doi:10.1016/j.asr.2013.03.007.
291. Tippenhauer N.O., Pöpper C., Rasmussen K.B., Capkun S. (2011) On the requirements for successful GPS spoofing attacks. Proceedings 18th ACM Conference on Computer and Communications Security (CCS '11), Chicago, Illinois, 75–86. doi:10.1145/2046707.2046719.
292. Bensky A. (2008) Wireless Positioning Technologies and Applications. GNSS Technology and Applications Series. Artech House Publishers, Boston, Massachusetts, USA.
293. UNOOSA (2018) The interoperable GNSS space service volume. United Nations Publication, Office for Outer Space Affairs United Nations Office at Vienna, Vienna, strane 1–108. https://www.unoosa.org/res/oosadoc/data/documents/2018/stspace/stspace75_0_html/st_space75E.pdf (21/02/2023).
294. Park Y., Kwon K.H., Won, J.H. (2017) Performance analysis of multi- constellation and multi-frequency GNSS receivers in deep space. Proceedings of the 30th international technical meeting of the satellite division of the institute of navigation (ION GNSS+ 2017), Portland, Oregon, USA, 1127–1132. doi:10.33012/2017.15138.
295. Ji G.-H., Shin H., Won J.-H. (2021) Analysis of multi-constellation GNSS receiver performance utilizing 1-st side-lobe signal on the use of SSV for KPS satellites. IET Radar Sonar Navig., 15, 485-499. doi:10.1049/rsn2.12052.
296. Yang J., Wang X., Shen L., Chen D. (2021) Availability analysis of GNSS signals above GNSSs constellation, The Journal of Navigation, 74(2), 446–466. doi:10.1017/S0373463320000594.
297. Lee H-B., Kwon K.-H., Won J.-H. (2022) Feasibility Analysis of GPS L2C Signals for SSV Receivers on SBAS GEO Satellites. Remote Sens. 14(21), 5329, 10 p. doi:3390/rs14215329.
298. Lombardi M.A., Nelson L.M., Novick A.N., Zhang V.S. (2001) Time and frequency measurements using the Global Positioning System. Cal. Lab. Int'l. J. Metrol., 8(3), 26–33. https://www.researchgate.net/publication/269280303_Time_and_Frequency_Measurements_Using_the_Global_Positioning_System (27/02/2023).
299. Penn State, College of Earth and Mineral Sciences, Pennsylvania. https://www.e-education.psu.edu/geog862/node/1861 (27/02/2023).
300. Badran-Taoglas B. (2022) Navigating the L1, L2 and L5 Band Options for GNSS. https://www.everythingrf.com/community/navigating-the-l1-l2-and-l5-band-options-for-gnss (27/02/2023)
301. Official U.S. government information about the Global Positioning System (GPS) and related topics. https://www.gps.gov/systems/gps/modernization/civilsignals/ (01/03/2023).
302. Warner J.S., Johnston R.G. (2002) A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. J. Secur. Admin., 25(2), 19–2.

ID:198960039. https://docplayer.net/17478079-A-simple-demonstration-that-the-global-positioning-system-gps-is-vulnerable-to-spoofing.html (27/02/2023).
303. Betz J. (2002) Binary offset carrier modulations for radionavigation. Navig. J. Inst. Navig., 48(4), 227–246. doi:10.1002/j.2161-4296.2001.tb00247.x.
304. Misra P., Enge P. (2011) Global Positioning System: Signals, Measurements, and Performance, Revised 2nd ed., Ganga-Jamuna Press, Lincoln, MA, USA. https://www.gpstextbook.com/ (27/02/2023).
305. Kaplan E.D., Hegarty J. (ed,) (2006) Understanding GPS: Principles and applications, 2nd ed., Artech House INC., MA, USA. https://d1.amobbs.com/bbs_upload782111/files_33/ourdev_584835O21W59.pdf (27/02/2023).
306. Alan Oxley (2017) GPS Modernization. In Uncertainties in GPS Positioning A Mathematical Discourse, 1st ed., Academic Press, Elsevier, Chapter 5, 71–80. doi:10.1016/B978-0-12-809594-2.00005-8.
307. Braasch M. S., van Dierendonck A. J. (1999) GPS receiver architectures and measurements. Proceedings IEEE, 87(1), 48–64. doi:10.1109/5.736341. https://ieeexplore.ieee.org/document/736341 (27/02/2023).
308. Digital Phase Modulation: BPSK, QPSK, DQPSK https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-modulation/digital-phase-modulation-bpsk-qpsk-dqpsk/ (27/02/2023).
309. Rebeyrol E., Macabiau C., Lestarquit L., Ries L., Issler J-L., Boucheret M.L., Bousquet M. (2005) BOC power spectrum densities. Proceedings of the National Technical Meeting of the Institute of Navigation, ION-NTM 2005, San Diego, California, USA, 769 –778. https://www.ion.org/publications/abstract.cfm?articleID=6042 (27/02/2023).
310. Hegarty C.J., Ligler G.T., Alexander K., Chesto L., Moses H., Wichgers J. M., Enge P., Erlandson B., Van Dierendonck A.J., Azoulai L., Kalyanaraman S., Heppe S., Lee J.C., Wesson K., Studenny J. (2015) RTCA SC-159: 30 Years of aviation GPS standards. *Proceedings* of the *28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, September 2015, 877–896. https://www.ion.org/publications/abstract.cfm?articleID=13133 (27/02/2023).
311. Bertz G. (2018) GNSS spoofing and aviation: An evolving relationship. Inside GNSS. https://insidegnss.com/gnss-spoofing-and-aviation-an-evolving-relationship/ (22/02/2023).
312. GSA (2018) Report on Aviation User Needs and Requirements, GNSS User Technology Report Issue 2, European GNSS Agency (GSA), Prague, Czechia. https://www.gsa.europa.eu/system/files/reports/gnss_user_tech_report_2018.pdf (01/02/2023).
313. ICAO (2018) Concept of Operations (CONOPS) for Dual-Frequency Multi-Constellation (DFMC) Global Navigation Satellite System (GNSS), CONOPS V6.4. https://www.icao.int/Meetings/anconf13/Documents/WP/Navigation_Systems_Panel_CONOPS_for_DFMC_GNSS.pdf (23/02/2023).
314. Zhai Y., Zhan X., Joerger M., Pervan B. (2019) Impact quantification of satellite outages on air navigation continuity. IET Radar Sonar Navig. 13(3), 376–383. doi:10.1049/iet-rsn.2018.5376.
315. SkyBrary (2020) Airborne Separation Assurance Systems (ASAS).

https://www.skybrary.aero/articles/airborne-separation-assurance-systems-asas (13/02/2023).
316. Enea G., Porretta M. (2012) A comparison of 4D-trajectory operations envisioned for NextGen and SESAR, some preliminary findings. Proceedings of the 28th International Congress of Aeronautical Sciences (ICAS 2012), Brisbane, Australia, Vol. 5, 4152–4165. http://toc.proceedings.com/16883webtoc.pdf (25/02/2023).
317. RTCA (2022) Paper No. 191-22/PMC-2307 Navigation Equipment Using the Global Navigation Satellite System (GNSS) (Version 20) https://www.rtca.org/wp-content/uploads/2022/06/SC-159-TOR-v20-Approved-2022-06-23.pdf (27/02/2023).
318. EUROCONTROL (2021) EUROCONTROL Voluntary ATM Incident Reporting (EVAIR) safety bulletin 20, for the period 2013–2017. EVAIR Safety Bulletin 20, EUROCONTROL, Brussels, Belgium. https://www.eurocontrol.int/publication/eurocontrol-voluntary-atm-incident-reporting-evair-safety-bulletin-20 (27/02/2023).
319. IATA (2018) Safety Report 2017, Issued April 2018. 54th edition, IATA, Montreal—Geneva. https://aviation-safety.net/airlinesafety/industry/reports/IATA-safety-report-2017.pdf (27/02/2023).
320. EUROCONTROL (2018) EUROCONTROL Voluntary ATM Incident Reporting (EVAIR) Bulletin No 19 for the period 2012–2016. https://eurocontrol.int/sites/default/files/publication/files/evair-bulletin-19.pdf (27/02/2023).
321. Buesnel G. (2018). Expect Your GPS to Be Trashed, GPS & ADS-B Problems at Manila Airport, RNT Foundation. https://rntfnd.org/2018/04/10/expect-yourgps-to-be-trashedgps-ads-b-problems-at-manila-airport/ (02/02/2023).
322. RNT Foundation, ed. (2017). Russian Exercise Jams Aircraft GPS in North Norway for a Week—NRK Translated from Norwegian, RNT Foundation. https://rntfnd.org/2017/10/05/russianexercise-jams-aircraft-gps-in-northnorway-for-a-week-nrk/ (27/02/2023).
323. Yle News (2018) Russia Suspected of GPS Jamming During Nato Exercises, YLE, Barents observer. https://yle.fi/a/3-10500210 (16/03/2023).
324. Brown A., Reynolds D., Roberts D., Serie S. (1999) Jammer and interference location system. in Proc. ION GPS, 137–142.
325. Simsky M. (2019) What is spoofing and how can you ensure GPS security? Aerospace testing international. https://www.aerospacetestinginternational.com/features/what-is-spoofing-and-how-can-you-ensure-gps-security.html (14/02/2023).
326. RTCA (2018) Operational Impacts of Intentional GPS Interference. Meeting Summary, March 1, 2018, Tactical Operations Committee (TOC), RTCA Paper No. 077-18 TOC-040. https://www.rtca.org/wp-content/uploads/2020/08/summary_mar_1_2018_toc_mtg_with_attch.pdf (18/02/2023).
327. Steindl E., Dunkel W., Hornbostel A., Haettich C., Remi P. (2013) The impact of interference caused by GPS repeaters on GNSS receivers and services Proceedings of the European Navigation Conference (ENC2013), Vienna. http://www.enc2013.org/ (28/02/2023).

328. GMCA 641613 White Paper (2016), Version 1.0, DW/02/001/096/032/1.0. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ae828ca9&appId=PPGMS (25/02/2023).
329. Norman S.M. (2019) Reliability and Trust in Global Navigation Satellite Systems. School of Electrical and Electronic engineering, University of Adelaide, Thesis for: Bachelor of Engineering, 2019.
330. International Telecommunication Union (ITU) (2016) Radio Regulations Articles. Edition of 2016, Vol. 1, ITU. https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.en.101.pdf (21/02/2023).
331. Novák A., Jun F., Škultéty F., Sedlačková A.N. (2019) Experiment demonstrating the possible impact of GNSS interference on instrument approach on RWY 06 LZZI. Transp. Res. Proc., 43, 74–83. doi:10.1016/j.trpro.2019.12.021.
332. Horton E., Prakash R. (2018) Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. J. Glob. Position. Syst. 16(9), 1–11. doi:10.1186/s41445-018-0018-3.
333. Turner M., Wimbush S., Enneking C, Konovaltsev A. (2020) Spoofing detection by distortion of the correlation function. Proceedings of the 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS), Portland, Oregon, USA, 566–574. doi:10.1109/PLANS46316.2020.9110173.
334. James J., Spilker Jr. James Axelrad P., Parkinson W.B., Enge P. (1996) Global positioning system: theory and Application, Vol. I, American Institute of Aeronautics and Astronautics, Inc., Washington, D.C., USA. doi:10.2514/4.866388
335. Olson Parmy, Forbes (2015) Hacking a phone's GPS may have just got easier. https://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/?sh=b1abbfb4efbf (10/01/2023).
336. Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner P.M. Jr. (2008) Assessing the spoofing threat: development of a portable GPS civilian spoofer. Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2008), Savanna, Georgia, USA, 2314–2325. https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf (10/01/2023).
337. Fernández-Hernández I., Walter T., Alexander K., Clark B., Châtre E., Hegarty C., Appel M., Meurer M. (2019) Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats. Proceedings of the ITM 2019: International Technical Meeting of The Institute of Navigation, Reston, Virginia, USA, 389–407. doi:10.33012/2019.16699.
338. Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W., Kintner P.M. Jr. (2008) Assessing the spoofing threat. Proceedings of the 21st Int. Tech. Meeting Satellite Div. Inst. Navig., 20, 28–38. https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf (15/02/2023).
339. Borowski H., Isoz O., Marsten F., Sherman Lo E., Akos D. (2012) Detecting false signals with automatic gain control. GPS World staff. https://www.gpsworld.com/detecting-false-signals-automatic-gain-control-12804/ (15/02/2023).
340. National PNT Advisory board comments on jamming the global positioning system (2010) A National security threat: recent events and potential cures, 1–10. https://techcrunch.com/wp-content/uploads/2011/03/2010-11-jammingwhitepaper.pdf (18/02/2023).

341. Nguyen T.X. NASA/TM-2004-213001 (2004) Evaluation of a mobile phone for aircraft GPS interference truong X. Nguyen Langley Research Center, Hampton, Virginia, USA, 1–12. https://www.cs.odu.edu/~mln/ltrs-pdfs/NASA-2004-tm213001.pdf (18/02/2023).
342. Wood A. (2011) Newark Airport GBAS Vulnerable to Truckers' GPS Jammers. https://www.ainonline.com/aviation-news/business-aviation/2011-01-25/newark-airport-gbas-vulnerable-truckers-gps-jammers (25/08/2022).
343. ICAO (2006) Annex 10 to the Convention on International Civil Aviation: Aeronautical Telecommuncations, Vol. 1, 6th edition, Radion Navigation Aids, ICAO, Montreal, QC, Canada, 2006. https://www.pilot18.com/wp-content/uploads/2017/10/Pilot18.com-ICAO-Annex-10-Volume-1-Radio-Navigation-Aids.pdf (25/08/2022).
344. Deshpande S.M. (2004) Study of Interference Effects on GPS Signal Acquisition. UCGE Reports Number 20199, University of Calgary, Department of Geomatics Engineering, Calgary, Alberta, Canada. https://schulich.ucalgary.ca/labs/position-location-and-navigation/files/position-location-and-navigation/deshpande2004_msc.pdf (21/02/2023).
345. Lee C.-M., Park K.-D., (2011) Generation of Klobuchar Ionospheric Error Model Coefficients Using Fourier Series and Accuracy Analysis, J. Astron. Space Sci. 28(1), 71–77.doi:10.5140/JASS.2011.28.1.071.
346. Jafarnia-Jahromi A., Broumandan A., Nielsen J., Lachapelle G. (2012) GPS vulnerability to spoofing threats and a review of antispoofing techniques. Int. J. Navig. Obs., 2012, 16 p. doi:10.1155/2012/127072.
347. Zheng Z., Luo X., Wu Z. (2012) Geometric Buildup Algorithms for Sensor Network Localization, Math. Probl. Eng., 2012, 18p. doi:10.1155/2012/927031.
348. Nguyen V.H., Falco G., Nicola M. Falletti E. (2018) A dual antenna GNSS spoofing detector based on the dispersion of double difference measurements. Proceedings of the 9th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC 2018), Noordwijk, Netherlands, 8p. doi:10.1109/NAVITEC.2018.8642705.
349. Rezaei M.J., Abedi M., Mosavi M.R. (2016) New GPS anti-jamming system based on multiple short-time Fourier transform. IET Radar Sonar Navig., 10(4), 807–815. doi:10.1049/iet-rsn.2015.0417.
350. Berz G. (2016) ICAO GNSS RFI Mitigation Plan and associated EUROCONTROL Efforts. UN ICG, Sochi, Russia. https://www.unoosa.org/pdf/icg/2016/icg11/wgs/6.pdf (18/02/2023).
351. Nava-Gaxiola L., Barrado C., Royo P. (2018) Study of a full implementation of free route in the European airspace. Proceedings of the IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 6p. doi:10.1109/DASC.2018.8569543.
352. Lucas-Sabola V., Seco-Granados G., López-Salcedo J.A., García-Molina J.A., Crisci M. (2016) Cloud GNSS receivers: New advanced applications made possible. Proceedings of the International Conference Localization and GNSS (ICL-GNSS), 6p. http://spcomnav.uab.es/docs/conferences/Lucas_ICL-GNSS_2016.pdf (17/02/2023).
353. Li W. Huang Z., Lang R., Qi H., Zhou K., Cao Y. (2016) A real-time interference monitoring technique for GNSS based on a twin support vector machine method. Sensors, 16(3), 329, 12 p. doi:10.3390/s16030329.

354. Linty N., Farasin A., Favenza A., Dovis F. (2019) Detection of GNSS ionospheric scintillations based on machine learning decision tree. IEEE Trans. Aerosp. Electron. Syst., 55(1), 303–317. doi:10.1109/TAES.2018.2850385.
355. Poudel S., Moh S. (2019) Medium access control protocols for unmanned aerial vehicle-aided wireless sensor networks: A survey. IEEE Access, 7, 65728–65744. doi:10.1109/ACCESS.2019.2917948.
356. Zhang J., Chen T., Zhong S., Wang J., Zhang W., Zuo X., Maunder R. G., Hanzo L. (2019) Aeronautical adhoc networking for the Internet-above-the-clouds. Proc. IEEE, 107(5), 868–911. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8710357 (17/02/2023).
357. Park P.. Di Marco P., Nah J., Fischione C. (2021) Wireless Avionics Intracommunications: A Survey of Benefits, Challenges, and Solutions. IEEE Internet Things J., 8(10), 7745-7767. doi:10.1109/JIOT.2020.3038848.
358. ITU-R (2010) Report ITU-R M.2197 Technical characteristics and operational objectives for wireless avionics intra-communications (WAIC). M Series Mobile, radiodetermination, amateur and related satellites services, 1–56. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2197-2010-PDF-E.pdf (17/02/2023).
359. Elgezabal Gomez O. (2010) Fly-by-wireless: Benefits, risks and technical challengesin. Proceedings of the CANEUS Fly-by-Wireless Workshop 2010, Orono, Maine, USA, 14–15. doi:10.1109/fbw.2010.5613788.
360. Aviation Pros (2008) Gulfstream demonstrates fly-by-wireless aircraft control system. https://www.aviationpros.com/home/press-release/10403052/gulfstream-demonstrates-flybywireless-aircraft-control-system (17/02/2023).
361. Pereira A., Lohmann G., Houghton L. (2022) Technology trajectory in aviation: Innovations leading to value creation (2000–2019). Int. J. Innov. Stud., 6(3), 128–141. doi:10.1016/j.ijis.2022.05.001.
362. Magdalena L. (2018) Designing interpretable Hierarchical Fuzzy Systems. Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Rio de Janeiro, Brazil, 894–901. doi:10.1109/FUZZ-IEEE.2018.8491452.
363. Yang F., Du M., Hu X. (2019) Evaluating Explanation Without Ground Truth in Interpretable Machine Learning. doi: 10.48550/arXiv.1907.06831. https://arxiv.org/pdf/1907.06831.pdf (12/02/2023).
364. Zadeh L. A. (1965) Fuzzy Sets. Inf. Control., 8(3), 338–353. doi:10.1016/S0019-9958(65)90241-X
365. Teodorović D., Kikuchi S., Uvod u teoriju fuzzy skupova i primene u saobraćaju, 2. izdanje, Saobraćajni fakultet Univerziteta u Beogradu, Beograd, 1994.
366. Milić D.S., Misović S.D., Ponjavić M.N. (2017) Primena teorije fazi logike za donošenje odluka u elektroenergetskom sektoru. Zbornik radova Infoteh–Jahorina, 16, 39–43. https://infoteh.etf.ues.rs.ba/zbornik/2017/radovi/ENS-1/ENS-1-1.pdf (28/02/2023)
367. Mamdani E.H. (1974) Application of Fuzzy Algorithm for Control of Simple Dynamic Plant. Proceedings of the Institution of Electrical Engineers, 121(12), 1585–1588. doi:10.1049/piee.1974.0328.
368. Takagi T., Sugeno M. (1983) Derivation of fuzzy control rules from human operator's control actions. IFAC Proceedings Volumes, 16(13), 55–60. doi:10.1016/S1474-6670(17)62005-6.
369. Zhang Y., Ishibuchi H., Wang S. (2018) Deep Takagi–Sugeno–Kang fuzzy classifier with shared linguistic fuzzy rules. IEEE Trans. Fuzzy Syst., 26(3), 1535–1549. doi:10.1109/TFUZZ.2017.2729507.

370. Kukolj D. (2002) Design of adaptive Takagi–Sugeno–Kang fuzzy models. Appl. Soft Comput., 2(2), 89–103. doi:10.1016/S1568-4946(02)00032-7.
371. Ho W. L., Tong W. L., Quek C., (2010) An evolving Mamdani-Takagi-Sugeno based neural-fuzzy inference system with improved interpretability-accuracy. Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ–IEEE), Barcelona, Spain, 8p. doi:10.1109/FUZZY.2010.5584831.
372. Lee C.C. (1990) Fuzzy logic in control systems: fuzzy logic controller. I. I*EEE Trans. Syst. Man Cybern. Syst*., 20(2), 404–418. doi**:**10.1109/21.52551.
373. Lee C.C. (1990) Fuzzy logic in control systems: fuzzy logic controller. II. I*EEE Trans. Syst. Man Cybern. Syst*., 20(2), 419–435. doi.10.1109/21.52552.
374. Kukolj D., Levi E. (2004) Identification of Complex Systems Based on Neural and Takagi-Sugeno Fuzzy Model, IEEE Trans. Syst. Man Cybern. Syst., Part B (Cybernetics), 34(1), 272–282. doi:10.1109/TSMCB.2003.811119.
375. Milić S.D., Vulević B.D., Stojić Đ.M. (2019) A Fuzzy-Measurement Algorithm for Assessing the Impact. Nucl. Technol. Radiat. Prot., 34(2), 129–137. doi:10.2298/NTRP190121018M.
376. Milić S.D., Miladinović N.M., Rakić A. (2020) A wayside hotbox system with fuzzy and fault detection algorithms in IIoT environment. Control Eng. Pract., 104, 104624. doi:10.1016/j.conengprac.2020.104624.
377. Radojičić N. (2018) Primena fazi logike za rešavanje NP-teških problema rutiranja vozila i lokacije resursa metodama računarske inteligencije, Doktorska disertacija, Univerzitet u Beogradu–Matematički fakultet, Beograd.
378. Ahmed S.K., Kabir G., Khan M.A., Haque A. (2019) Fuzzy Logic Application for Aircraft Landing Performance Analysis. Proceedings of the 2nd International Conference on Industrial and Mechanical Engineering and Operations Management (IMEOM), Dhaka, Bangladesh, 247–252. http://www.ieomsociety.org/imeom/81.pdf (18/02/2023). (10/02/2023).
379. Roopashree S., Deepika K.M., Bhat S. (2012) Design and Implementation of Fuzzy Controller for Estimating the Attitude of Unmanned Aerial Vehicles. In Das V. V., Ariwa E., Rahayu S.B. (eds.): Signal Processing and Information Technology, Proceedings of the First International Joint Conference, SPIT 2011, Amsterdam, Netherlands, 255–261. https://eudl.eu/pdf/10.1007/978-3-642-32573-1_43 (18/02/2023).
380. Torres A., Nieto J.J. (2006) Fuzzy Logic in Medicine and Bioinformatics. J Biomed. Biotechnol., 2006(2), 1–7. doi:10.1155/JBB/2006/91908.
381. Sanchez-Roger M., Oliver-Alfonso M.D., Sanchís-Pedregosa C. (2019) Fuzzy logic and its uses in finance: a systematic review exploring its potential to deal with banking crises. Mathematics 7(1), 1091. doi:10.3390/math7111091.
382. Pamučar S.D., Vasin T. Lj., Đorović D.B., Lukovac M.V. (2012) Dizajniranje organizacione structure upravnih organa logistike korišćenjem fuzzi pristupa. Vojnotehnički glasnik/Mil.Tech.Cour., 60(3), 143–167. doi:10.5937/vojtehg1203143P.
383. Pešić A., Pešić D., Ivković S. (2014) Lingvističke fazi promenljive kao alat analize u menadžmentu inventara. FBIM Transactions, 2(2), 258–270. doi:10.12709/fbim.02.02.02.26.
384. Gu X., Han J., Shen Q., Angelov P.P. (2022) Autonomous learning for fuzzy systems: a review. Artif. Intell. Rev., 47 p. doi:10.1007/s10462-022-10355-6.
385. Shihabudheen K.V., Pillai G.N. (2018) Recent advances in neuro-fuzzy system: A survey, Knowledge–Based Systems, 152(C), 136–162. doi:10.1016/j.knosys.2018.04.014.

386. Terziyska M., Terziyska Z. (2020) Computationally efficient neuro-fuzzy predictive models. Int. J. Technol. Manag., 1(2), 19–24. https://journal.iiit.bg/wp-content/uploads/2020/08/3_COMPUTATIONALLY-EFFICIENT-NEURO-FUZZY-PREDICTIVE-MODELS.pdf (18/02/2023).
387. Jang J.-S.R. (1993) ANFIS: adaptive-network-based fuzzy inference system. IEEE Trans. Syst. Man Cybern., 23(3), 665–685. doi:10.1109/21.256541.
388. Bherenji H.R., Khedkar P. (1992) Learning and Tuning Fuzzy Logic Controllers through Reinforcements. IEEE Trans. Neural Netw., 3(5), 724–740. doi:10.1109/72.159061.
389. Nauck D., Klawonn F., Kruse R. (1997) Foundations of neuro-fuzzy systems. John Wiley & Sons, Inc, New York, NY, USA.
390. Ahmed M.H., Samsudin K., Ramli A.R. (2011) Optimizing of ANFIS for estimating INS error during GPS outages. J. Chin. Inst. Eng., 34(7), 967–982. doi:10.1080/02533839.2011.591970.
391. Ubeyli E.D. (2009) Adaptive Neuro-Fuzzy Inference Systems for Automatic Detection of Breast Cancer. *J. Med. Syst.*, 33(5), 353–358. doi:10.1007/s10916-008-9197-x.
392. Kambalimath S., Deka P.C. (2020) A basic review of fuzzy logic applications in hydrology and water resources. Appl. Water Sci., 10(8), 191, 14 p. doi:10.1007/s13201-020-01276-2.
393. Suganthi L., Iniyan S., Samuel A.A. (2015) Applications of fuzzy logic in renewable energy systems – A review. Renew. Sustain. Energy Rev., 48, 585–607. doi:10.1016/j.rser.2015.04.037.
394. Gharajeh M.S., Jond H.B. (2020) Hybrid Global Positioning System-Adaptive Neuro-Fuzzy Inference System based autonomous mobile robot navigation. Robot. Auton. Syst., 134(3), 103669. doi:10.1016/j.robot.2020.103669.
395. Sun J., Ellerbroek J., Hoekstra J. (2017) Flight Extraction and Phase Identification for Large Automatic Dependent Surveillance–Broadcast Datasets. J. Aerosp. Inf. Syst., 14(10), 566–572. doi:10.2514/1.I010520.
396. Żyluk A., Kuźma K., Grzesik N., Zieja M., Tomaszewska J. (2021) Fuzzy Logic in Aircraft Onboard Systems Reliability Evaluation–A New Approach. Sensors. 21(23), 7913. doi:10.3390/s21237913.
397. Hiliuta A., Landry R., Gagnon F. (2004) Fuzzy corrections in a GPS/INS hybrid navigation system**.** IEEE Trans. Aerosp. Electron. Syst., 40(2), 591–600. doi:10.1109/TAES.2004.1310007.
398. Mudheher A.H., Samsudin K., Ramli A.R. (2012) GPS/INS Integration Based on Dynamic ANFIS Network, *Int. J. Control Autom.*, 5(3), 21 p.
399. Sun R., Hsu L.-T., Xue D., Zhang G., Ochieng W.Y. (2019) GPS Signal Reception Classification Using Adaptive Neuro-Fuzzy Inference System. J. Navig., 72(3), 685–701. doi:10.1017/S0373463318000899.
400. Reznik L., Ghanayem O., Bourmistrov A. (2000) PID plus fuzzy controller structures as a design base for industrial applications. Eng. Appl. Artif. Intell., 13(4), 419–430. doi:10.1016/S0952-1976(00)00013-0.
401. Jenab K., Pineau J. (2018) Automation of Air Traffic Management Using Fuzzy Logic Algorithm to Integrate Unmanned Aerial Systems into the National Airspace. Int. J. Electr. Comput. Eng., 8(5), 3169–3178. doi:10.11591/ijece.v8i5.pp3169-3178.
402. Pasieka M., Grzesik N., Kuźma K. (2016) Simulation modeling of fuzzy logic controller for aircraft engines. *Int. J. Comput.*, 16(1), 27–33.

403. Sun J., Ellerbroek J., Hoekstra J. (2016) Large-scale flight phase identification from ADS-B data using machine learning methods. Proceedings of the 7th International Conference on Research in Air Transportation (ICRAT 2016), Drexel University, Philadelphia, USA, 7 p. https://drive.google.com/file/d/1y1onriehlUQujQTnpyT_3q7qQIEYDbIN/view (12/02/2023).
404. Flight Global (2019) Why ADS-B technology could drive air traffic revolution. https://www.flightglobal.com/opinion/why-ads-b-technology-could-drive-air-traffic-revolution/132627.article (01/03/2023).
405. Minesota Historical Society. https://www.mnhs.org/lindbergh/learn/aviation/commercial (01/03/2023).
406. Industry High Level Group (IHLG) (2019) Aviation Benefits Report, 76 p. https://www.icao.int/sustainability/Documents/AVIATION-BENEFITS-2019-web.pdf (01/03/2023).
407. FAA (2016) FAA Aerospace Forecast Fiscal Years 2016-2036. Federal Aviation Administration, 91 p. https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/fy2016-36_faa_aerospace_forecast.pdf (01/03/2023).
408. https://www.gettyimages.com/detail/news-photo/charles-august-lindbergh-american-pilot-with-his-wife-1932-news-photo/545031287?adppopup=true (01/03/2023).
409. RTCA (2002) Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B). RTCA DO-242A, RTCA Special Committee 186, Washington D.C., USA, 221 p.
410. EUROCONTROL (2011) Coding Rules for "Reserved Expansion Field" for ASTERIX Category 021. European Air Traffic Management, 16 p. https://www.eurocontrol.int/sites/default/files/2019-06/appendixcat021pt12aed11.pdf (01/03/2023). (01/03/2023).
411. FAA (2010) Automatic Dependent Surveillance Broadcast (ADS-B) Out performance requirements to support Air Traffic Control (ATC) service, Final Rule. Part III Department of Transportation Federal Aviation Administration, 14 CFR Part 91, Federal Register 75 (103), 30159-30195 https://www.govinfo.gov/content/pkg/FR-2010-05-28/pdf/2010-12645.pdf (01/03/2023).
412. FAA (2017) Automatic dependent surveillance – broadcast (ADS-B). https://www.faa.gov/air_traffic/technology/adsb/ (01/03/2023). (11/02/2023).
413. McCallie, D., Butts J., Mills R. (2011) Security Analysis of The ADS-B Implementation in the Next Generation Air Transportation System. Int. J. Crit. Infrastruct. Prot., 4(2), 78–87. doi:10.1016/j.ijcip.2011.06.001.
414. Purton L., Abbass H., Alam S. (2010) Identification of ADS-B system vulnerabilities and threats. Proceedings of the Australasian Transport Research Forum 2010, Canberra, Australia, 16 p. http://atrf.info/papers/2010/2010_purton_abbass_alam.pdf (01/03/2023).
415. Semke W., Allen N., Tabassum A., McCrink M., Moallemi M., Snyder K., Arnold E., Stott D., Wing M.G. (2017) Analysis of Radar and ADS-B Influences on Aircraft Detect and Avoid (DAA) Systems. Aerospace 4(3), 49, 14 p. doi:10.3390/aerospace4030049.
416. Du L., Liu H., Bao Z., Zhang J. (2007) Radar automatic target recognition using complex high-resolution range profiles. IET Radar Sonar Navigat., 1(1), 18–26. doi:10.1049/iet-rsn:20050119.

417. Richards M.A., Scheer J.A., Holm W.A. (eds.) (2010) Principles of Modern Radar: Basic Principles. SciTech Publishing: Raleigh, NC, USA.
418. ICAO (2004) Doc. 9684 AN/951: Manual on the Secondary Surveillance Radar (SSR) Systems, 3rd ed., ICAO, Montreal, QC, Canada. https://vdocuments.mx/doc-9684-ssr.html (01/03/2023). (01/02/2023).
419. Strohmeier M., Martinovic I., Lenders V. (2020) Chapter: Securing the Air-Ground Link in Aviation. In (ed.) Keupp M. M.: The Security of Critical Infrastructures: Risk, Resilience and Defense, 1st ed, Springer, Oxford, U. K., 31–154. https://www.cs.ox.ac.uk/files/13226/chapter-revision.pdf (01/03/2023).
420. ICAO (2020) Doc. 9924: Aeronautical Surveillance Manual, 3rd ed., ICAO, Montreal, QC, Canada.
421. Leonardi M., Piracci E., Galati G. (2017) ADS-B jamming mitigation: a solution based on a multichannel receiver. IEEE Aerosp. Electron. Syst. Mag., 32(11), 44-51. doi:10.1109/MAES.2017.160276.
422. McLean D. (2003) Operational Requirements for Fully Automatic Flight. Aircr. Eng. Aerosp. Technol., 75(6), 570–574. doi:10.1108/00022660310503039.
423. Romli F. I., King J. D., Li L., Clarke, J. P. (2008) Impact of Automatic Dependent Surveillance – Broadcast (ADS-B) on Traffic Alert and Collision Avoidance System (TCAS) Performance. Proceedings of AIAA Guidance, Navigation and Control Conference and Exhibit, Honolulu, Hawaii, USA. doi:10.2514/6.2008-6971.
424. Sjödin A., Gruenau M. (2020) The ADS-B protocol and its' weaknesses: exploring potential attack vectors. Examensarbete inom teknik, grundnivå, 15 HP Stockholm, Sverige, 2020, 43p. https://www.diva-portal.org/smash/get/diva2:1464430/FULLTEXT01.pdf (01/03/2023).
425. FAA, ADS-B In Pilot Applications. https://www.faa.gov/air_traffic/technology/adsb/pilot (20/01/2023).
426. Schäfer M., Lenders V., Martinovic I. (2013) Experimental analysis of attacks on next generation air traffic communication. Applied Cryptography and Network Security: Proceedings of the 11th International Conference ACNS 2013, Banff, Canada, 2013, 253–271. LNSC vol. 7954. Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-38980-1_16.
427. Ghose N., Lazos L. (2015) Verifying ADS-B navigation information through Doppler shift measurements. Proceedings of the IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, Czech Republic, 4A2-1–4A2-11. doi:10.1109/DASC.2015.7311412.
428. RTCA (2009) Minimum operational performance standards for 1090 MHz extended squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B). DO-260B (with Corrigendum 1), RTCA Inc., Washington, D.C., USA. http://www.anteni.net/adsb/Doc/1090-WP30-18-DRAFT_DO-260B-V42.pdf (01/03/2023).
429. Musmann F. (2018) ADS–B and Functions for Flight Inspection, Proceedings of the 2018 International Flight Inspection Symposium, Monterey, California, April 16-20, 2018, 111–123. http://www.icasc.co/sites/faa/uploads/documents/20th_IFIS_Papers/Papers/IFIS18-0010.pdf (22/02/2023).
430. Strohmeier M., Olive X., Lübbe J., Schäfer C., Lenders V. (2021), Crowdsourced air traffic data from the OpenSky network 2019–2020. Earth Syst. Sci. Data., 13(2), 357–366. doi:10.5194/essd-13-357-2021.

431. Akyüz M.K. (2022) Environmental and enviroeconomic impacts of COVID-19 pandemic on commercial flights. Aircr. Eng. Aerosp. Technol., 94(8), 1449–1457. doi:10.1108/AEAT-03-2022-0073.
432. Karunakaran C.S., Ashok Babu J. (2022) Impact of human factors in aircraft accident mitigation and aircraft maintenance training needs in post COVID-19 aviation. Aircr. Eng. Aerosp. Technol., 94(8) 1296–1302. doi:10.1108/aeat-10-2021-0300.
433. Miller S., Moat H.S., Preis T. (2020) Using aircraft location data to estimate current economic activity. Sci. Rep.,10(1), 7576–7583. doi:10.1038/s41598-020-63734-w.
434. Sun J., Olive X., Strohmeier M., Chafer M., Martinovic I., Lenders V. (2021) OpenSky report 2021: insights on ADS-B mandate and fleet deployment in times of crisis. Proceedings of the IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, *Texas*, USA, 10 p. doi:10.1109/DASC52595.2021.9594361.
435. SESAR (2021), Automatic Dependent Surveillance – Broadcast. https://www.sesarju.eu/sites/default/files/documents/reports/SESAR%20Solutions%20Catalogue%202021%20small.pdf (12/08/2022).
436. Flight Safety Foundation (2016) Benefits Analysis of Space-Based ADS-B, 38 p. https://flightsafety.org/wp-content/uploads/2016/10/ADS-B-report-June-2016-1.pdf (01/03/2023). (10/01/2023).
437. Bellamy III W. (2021) FAA works on latest ADS-B challenges and opportunities, Version 3, new ADS-B In applications and fixing the call sign mismatch problem. Avionics International, 2021. http://interactive.aviationtoday.com/avionicsmagazine/august-september-2021/faa-works-on-latest-ads-b-challenges-and-opportunities/ (01/03/2023).
438. Bellamy III W. (2021) What's next for ADS-B in the US air traffic system? Avionics International, 2021. http://interactive.aviationtoday.com/avionicsmagazine/august-september-2021/whats-next-for-ads-b-in-the-us-air-traffic-system/ (01/03/2023).
439. Xu Y., Yang J., Liu K., Guo J., Ma J., He Y. (2015), Research and WebGIS based system design of flight monitoring based on ADS-B. Proceedings of the International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2015), Atlantis Press, 111–118. doi:10.2991/ameii-15.2015.19.
440. Kunzi F., Hansman J. R. (2011) ADS-B benefits to general aviation and barriers to implementation, Report No. ICAT – 2011-6, MIT International Center for Air Transportation (ICAT), Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, USA, 103 p. https://dspace.mit.edu/bitstream/handle/1721.1/63130/Kunzi-ICAT-Report.pdf (01/03/2023).
441. ICAO (2014) Doc. 9994 AN/496: Manual on Airborne Surveillance Applications, 1st ed. http://icscc.org.cn/upload/file/20190102/Doc.9994-EN%20Manual%20on%20Airborne%20Surveillance%20Applications.pdf (11/03/2023).
442. Kraemer A.D., Villani E., Arjoni D.H., (2019) Aircraft FDI and human factors analysis of a take-off maneuver using SIVOR flight simulator. IFAC–PaperOnLine, 51(34), 184–189. doi:10.1016/j.ifacol.2019.01.063.
443. Silva S.S., Cho H., Hansman R.J. (2014) Human factors studies of an ADS-B based traffic alerting system for general aviation. Proceedings of the 29th Congress of the International Council of the Aeronautical Sciences (ICAS 2014), St. Petersburg, Russia, 10p. https://dspace.mit.edu/handle/1721.1/77116 (12/03/2023)

444. Isaković V., Đurđević D. (2021) Zamor kao pretnja u civilnom vazduhoplovstvu. Megatrend revija, 18(1), 105–124. doi:10.5937/MegRev2101105I.
445. Magazu D. III. (2012) Exploiting the Automatic Dependent Surveillance-Broadcast System Via False Target Injection. Theses and Dissertations. 1132. https://scholar.afit.edu/etd/1132 (01/03/2023).
446. How Airbus defends against 12 big cyber attacks each year, http://www.itnews.com.au/news/howairbus-defends-against-12-big-cyber-attacks-each-year-418131 (02/03/2023).
447. Haas J., Hu Y., Laberteaux K. (2009) Real-world VANET security protocol performance. Proceedings of the 28th IEEE Global Telecommunications Conference (GLOBECOM'09), Honolulu, Hawaii USA, 2629–2635. https://dl.acm.org/doi/10.5555/1811681.1811817#d30140212e1 (02/03/2023).
448. Ronen R., Ben-Moshe B. (2021) Cyberattack on flight safety: detection and mitigation using LoRa. Sensors, 21(13), 4610, 16 p. doi:10.3390/s21134610.
449. Leonardi M., Di Gregorio L., Di Fausto D. (2017) Air traffic security: aircraft classification using ADS-B messages phase-pattern. Aerospace, 4(4), 51, 13 p. doi:10.3390/aerospace4040051.
450. Chan-Tin E., Heorhiadi V., Hopper N., Kim Y. (2011) The frog-boiling attack: limitations of secure network coordinate systems. ACM Trans. Inf. Syst. Secur., 14(3), 1–23. doi:10.1145/2043621.2043627.
451. Strohmeier M., Lenders V., Martinovic I. (2015) On the security of the automatic dependent surveillance-broadcast protocol. IEEE Commun. Surv. Tutor., 17(2), 1066–1087. doi:10.1109/COMST.2014.2365951.
452. Mirzaei K. F., de Carvalho B. P., Pschorn P. (2019) Security of ADS-B: attack scenarios. EasyChair Preprint No. 851, 8 p. https://doi.org/10.29007/dd4b.
453. Sampigethaya K., Poovendran R., Shetty S., Davis T., Royalty C. (2011) Future e-enabled aircraft communications and security: the next 20 years and beyond. Proceedings of the *Institute of Electrical and Electronics Engineers (*IEEE), 99(11), 2040–2055. doi:10.1109/JPROC.2011.2162209.
454. Gurtov A., Polishchuk T., Wernberg M. (2018) Controller–pilot data link communication security. Sensors, 18(5), 1636, 12p. doi:10.3390/s18051636.
455. Leonardi M., Sirbu G. (2021) ADS–B crowd-sensor network and two-step Kalman filter for GNSS and ADS-B cyber-attack detection. Sensors, 21(15), 4992, 18p. doi:10.3390/s21154992.
456. Mink D.M, McDonald J., Bagui S., Glisson W.B., Shropshire J., Benton R., Russ S. (2021) Near-real-time IDS for the U.S. FAA's NextGen ADS-B. *Big Data Cogn. Comput.*, 5(2), 27, 15 p. doi:10.3390/bdcc5020027.
457. Chan-Tin E., Feldman D., Hopper N., Kim Y. (2009) The frog-boiling attack: limitations of secure network coordinate systems. In Chen Y., Dimitriou T. D., Zhou J. (eds.): Security and Privacy in Communication Networks, Proceeding of the International Conference on Security and Privacy in Communication System SecureComm 2009, Athens, Greece, 448–458. LNICST vol. 19, Springer, Berlin, Heidelberg, doi:10.1007/978-3-642-05284-2_26.
458. Pöpper C., Tippenhauer N.O., Danev B., Capkun S. (2011) Investigation of Signal and Message Manipulations on the Wireless Channel. Proceeding of the 16th European conference on Research in computer security (ESORICS 2011), Leuven, Belgium, 40–59. LNSC vol. 6879. Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-23822-2_3.
459. Wilhelm M.S., Schmitt J.B., Lenders V. (2012) Practical message manipulation attacks in IEEE 802.15.4 wireless networks. Workshop Proceedings of the 16th

International GI/ITG Conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance. MMB & DFT 2012, Kaiserslautern, Germany, 29–31. https://www.academia.edu/7467382/Practical_Message_Manipulation_Attacks_in_IEEE_802_15_4_Wireless_Networks (02/03/2023).

460. Wu Z., Shang T., Guo A. (2020) Security Issues in Automatic Dependent Surveillance – Broadcast (ADS-B): A Survey. IEEE Access, 8, 122147–122167. doi:10.1109/ACCESS.2020.3007182.
461. Wesson K. D., Humphreys T. E., Evans B. L. (2014) Can cryptography secure next generation air traffic surveillance? IEEE Security&Privacy, 10, 8 p. https://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf (02/03/2023).
462. Alghamdi F., Alshrahani A., Hamza N. (2018) Effective security techniques for automatic dependent surveillance-broadcast (ADS-B), Int. J. Comput. Appl., 180(26), 23–28. doi:10.5120/ijca2018916598.
463. Perrig A., Canetti R., Tygar J. D., Song D. (2002) The TESLA Broadcast Authentication Protocol. CryptoBytes, 5(2), Summer/Fall 2002, 2–13. https://people.eecs.berkeley.edu/~tygar/papers/TESLA_broadcast_authentication_protocol.pdf (02/03/2023).
464. Kalman R. E. (1960) A New Approach to Linear Filtering and Prediction Problems. J. Basic Eng., 82(1), 35–45. doi:10.1115/1.3662552.
465. Fox V., Hightower J., Liao L., Schulz D., Borriello G. (2003) Bayesian Filters for Location Estimation. IEEE Pervasive Comput., 2(3), 24–33. doi:10.1109/MPRV.2003.1228524.
466. Farid Z., Nordin R., Ismail M. (2013) Recent Advances in Wireless Indoor Localization Techniques and System. J. Comput. Netw. Commun., 2013, 12p. doi:10.1155/2013/185138.
467. Herrero J. J., Portas J., Corredera J. R. C., Besada Portas J., Rodriguez F. (1999) ASDE and Multilateration Mode-S Data Fusion for Location and Identification on Airport Surface. Proceedings of the 1999 IEEE Radar Conference. Radar into the Next Millennium, Waltham, Massachusetts, USA, 315–320. doi:10.1109/NRC.1999.767354.
468. Nijsure Y.A., Kaddoum G., Gagnon G., Gagnon F., Yuen C., Mahapatra R. (2016) Adaptive Air-to-Ground Secure Communication System Based on ADS-B and Wide-Area Multilateration. IEEE Trans. Veh. Technol., 65(5), 3150–3165. doi:10.1109/tvt.2015.2438171.
469. Sampigethaya K., Poovendran R. (2011) Security and Privacy of Future Aircraft Wireless Communications with Offboard Systems. Proceedings of the 3rd International Conference on Communication Systems and Networks (COMSNETS 2011), Bangalore, India, 6 p. doi:10.1109/COMSNETS.2011.5716527.
470. Baud O., Honore N., Taupin O. (2006) Radar/ADS-B Data Fusion Architecture for Experimentation Purpose. Proceedings of the 9th International Conference on Information Fusion, Florence, Italy, 6p. doi:10.1109/ICIF.2006.301555.
471. Liu W., Wei J., Liang M., Cao Y., Hwang I. (2013) Multi-Sensor Fusion and Fault Detection Using Hybrid Estimation for Air Traffic Surveillance. IEEE Trans. Aerosp. Electron. Syst., 49(4), 2323–2339. doi:10.1109/TAES.2013.6621819.
472. Yong T., Honggang W., Zhili X. Zhongtao H. (2012) ADS-B and SSR Data Fusion and Application. Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE2012)., Zhangjiajie, China, 2, 255–258. doi:10.1109/CSAE.2012.6272769.

473. Habler E., Shabtai A. (2018) Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages, Comput Secur., 78, 155–173. doi:org/10.1016/j.cose.2018.07.004.
474. Darabseh A., AlKhzaimi H., Pöpper C. (2020) MAVPro: ADS-B message verification for aviation security with minimal numbers of on-ground sensors. Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), Virtual event, Linz, Austria, 53–64. doi:10.1145/3395351.3399361.
475. Finke C., Butts J., Mills R., Grimaila M.R. (2013) Enhancing the security of aircraft surveillance in the next generation air traffic control system. Int. J. Crit. Infrastruct. Prot., 6(1), 3–11. doi:10.1016/j.ijcip.2013.02.001.
476. Schafer, M., Lenders, V., Schmitt, J. (2015) Secure track verification. Proceedings of the *IEEE Symposium on Security and Privacy* (SP2015), San Jose, *California*, USA, 199–213. doi:10.1109/SP.2015.20.
477. Schafer M., Lenders V., Schmitt J. (2016). Secure motion verification using the Doppler effect. Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '16), Darmstadt Germany, 135–145. doi:10.1145/2939918.2939920.
478. Moore J. (2016) ADS-B for drones: Tiny transceiver developed. Aircraft Owners and Pilots Association. https://www.aopa.org/news-and-media/all-news/2016/may/04/nextgen-for-drones (02/03/2023).
479. Gontar P., Homans H., Rostalski M., Behrend J., Dehais F., Bengler K. (2018) Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior. J. Air Transp. Manag., 69, 26–37. doi:0.1016/j.jairtraman.2018.01.004.
480. Smith M., Strohmeier M., Harman J., Lenders V., Martinovic I. (2020) A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems. Proceedings of Network and Distributed Systems Security (NDSS) Symposium 2020, San Diego, *California*, USA. doi:10.14722/ndss.2020.23022.
481. Byers J. C., Bittner A. C., Hill S. G. (1989). Traditional and raw task load index (TLX) correlations: are paired comparisons necessary? In Mital A. (ed.): Advances in Industrial Ergonomics and Safety I. Taylor & Francis, New York, NY, 481–485.
482. Gold C., Körber M., Hohenberger C., Lechner D., Bengler K. (2015). Trust in automation – before and after the experience of take-over scenarios in a highly automated veshicle. Proc. Manuf., 3, 3025–3032. doi:10.1016/j.promfg.2015.07.847.
483. Spain R.D., Bustamante E.A., Bliss J.P. (2008) Towards an empirically developed scale for system trust: take two., Proc. Hum. Factors Ergon. Soc. Annu. Meet., 52(19), 1335–1339. doi:10.1177/154193120805201907.
484. Jian J.-Y., Bisantz A.M., Drury C.G. (2000) Foundations for an empirically determined scale of trust in automated systems. Int. J. Cognit. Ergon., 4(1), 53–71. doi:10.1207/S15327566IJCE0401_04.
485. IFALPA (2013) Cyber Threats: Who Controls Your Aircraft? Positions, 14POS03. http://www.anpac.it/attachments/article/575/130605-IFALPA-Cyber%20threats%20who%20controls%20your%20aircraft.pdf (02/03/2023).
486. ICAO (2016) Working Paper. Coordinating Cybersecurity Work. A39-WP/2361 TE/91 Revision No. 1. Montreal, QC, Canada, 2016. https://www.icao.int/Meetings/a39/Documents/WP/wp_236_rev1_en.pdf (02/03/2023).

487. Peryer G., Noyes J., Pleydell-Pearce K., Lieven N. (2005). Auditory alert characteristics a survey of pilot views. Int. J. Aviat. Psychol., 15(3), 233–250. doi:10. 1207/s15327108ijap1503_2.
488. Mumaw R.J. (2017) Analysis of alerting system failures in commercial aviation accidents. Proc. Hum. Factors Ergon. Soc. Annu. Meet., 61 (1), 110–114. doi:10. 1177/1541931213601493.
489. Firesmith D. (2018) Common concepts underlying safety, security, and survivability engineering. Carnegie Mellon University. Report. https://doi.org/10.1184/R1/6572621.v1 https://doi.org/10.1184/R1/6572621.v1.
490. Gontar P., Schneider S.A.E., Schmidt-Moll C., Bollin C., Bengler K. (2017) Hate to interrupt you, but… analyzing turn-arounds from a cockpit perspective. Cogn. Tech. Work, 19, 837–853. doi:10.1007/s10111-017-0440-4.
491. Linkov V, Zámecník P, Havlícková D., Pai C.-W. (2019) Human Factors in the Cybersecurity of Autonomous Vehicles. Trends in Current Research. Front. Psychol., 10, 995, 7p. doi:10.3389/fpsyg.2019.00995.
492. Satterfield K., Mancuso V.F., Strang A., Greenlee E., Miller B., Funke G.J. (2018) When actions speak louder than words: Using changes in operator behavior and system efficiency measures to detect the presence of a cyber attack. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 62(1), 270–271. doi:10.1177/1541931218621062.
493. Garcia A.B., Babiceanu R.F., Seker R. (2021) Artificial intelligence and machine learning approaches for aviation cybersecurity: an overview. *Integrated Communications Navigation and Surveillance Conference (ICNS2021)*, Dulles, Virginia, USA, 8 p. doi:10.1109/ICNS52807.2021.9441594.
494. Airline Routes& Graund Servuces (ARGS). Darhttps://airlinergs.com/darktrace-signs-multi-million-dollar-deal-with-top-global-airline/ (02/03/2023).
495. Darktrace Blog (2022) Piloting Airline Cyber Security with AI https://darktrace.com/blog/piloting-airline-cyber-security-with-ai (02/03/2023).
496. Ukwandu E. Ben-Farah M.A., Hindy H., Bures M., Atkinson R., Tachtatzis C., Andonovic I., Bellekens X. (2022) Cyber-Security challenges in aviation industry: a review of current and future trends, Information 13(3), 146–167. doi:10.3390/info13030146.
497. Viveros C. A. P. (2016) Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts, Master's Thesis, University of Tartu, Institute of Computer Science, Estonia.
498. Riley C., Cerchio, D.R. (2011) Aircraft Systems Cyber Security. Proceedings IEEE/AIAA 30th Digital Avionics Systems Conference (DASC), Seattle, Washington, USA, 1C3-1–1C3-7. doi:10.1109/ICNSurv.2012.6218454.
499. Gross G. (2003) FAA: Slammer Didn't Hurt Us, but Other Attacks Coming. https://www.networkworld.com/article/2339600/faa--slammer-didn-t-hurt-us--but-other-attacks-coming. html (25/02/2023).
500. Goodin D. (2009) US Air Traffic Faces 'Serious Harm' from Cyber Attackers. https://www.theregister.com/20 09/05/07/air-traffic-cyber-attack/ (25/02/2023).
501. ICAO (2012) Working Paper. ICAO 12th Air Navigation Conference (AN-Conf/12), Montréal, Canada, 2012. https://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP130.2.1.ENonly.pdf (25/02/2023).
502. Paganini P. (2013) Istanbul Ataturk International Airport Targeted by a Cyber-Attack.

https://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html (25/02/2023).
503. Welsh W. (2014) Phishing Scam Targeted 75 US Airports. https://www.informationweek.com/cybersecurity/phishing-scam-targeted-75-us-airports (25/02/2023).
504. Reuters, World News (2014) Jets vanishing from Europe radar linked to war games. https://www.reuters.com/article/uk-europe-airplanes-safety-idUKKBN0EO1CO20140613 (25/02/2023).
505. Brewster T. (2015) Attack On LOT Polish Airline Grounds 10 Flights. https://www.forbes.com/sites/thomasbrewster/2015/06/22/lot-airline-hacked/?sh=3ca8f39e124e (25/02/2023).
506. Valero J. (2016) Hackers bombard aviation sector with over 1,000 attacks per month. https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/ (25/02/2023).
507. Kirkliauskaite K. (2020) Main Cyber-Security Challenges in Aviation. https://www.aerotime.aero/articles/25150-main-cyber-security-challenges-in-aviation (25/02/2023).
508. Polityuk P. Prentice A. (2016) Ukraine Says to Review Cyber Defenses after Airport Targeted from Russia. https://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0 (25/02/2023).
509. Pearson J. (2022) Ukraine launches 'IT army,' taking aim at Russian cyberspace. https://www.breakingnews.ie/ukraine/ukraine-launches-it-army-takes-aim-at-russian-cyberspace-1265233.html (25/02/2023).
510. Sandle P. (2018) British Airways Says 'Sophisticated' Hacker Stole Data on 380,000 Customers. https://www.insurancejournal.com/news/international/2018/09/10/500566.htm (25/02/2023).
511. Park K. Hong H. (2018) Cathay Pacific Cyber Attack Is World's Biggest Airline Data Breach. https://www.insurancejournal.com/news/international/2018/10/26/505699.htm (25/02/2023).
512. Singh K. (2018) Delta, Sears Report Data Breach by Service Provider. https://www.insurancejournal.com/new s/national/2018/04/05/485440.htm (25/02/2023).
513. Leyden J. (2018) Brit Airport Pulls Flight info System Offline after Attack by 'Online Crims'. https://www.theregister.com/2018/09/17/bristol-airport-cyber-attack/ (25/02/2023).
514. Sandle T. (2018) Air Canada Suffers Major App Data Breach of 20,000 Customers. https://www.digitaljournal.com/business/air-canada-in-major-app-data-breach/article/530763 (25/02/2023).
515. Gibbs B. (2018) Potential Personally Identifiable Information (PII) Compromise of NASA Servers. https://spaceref.com/status-report/potential-personally-identifiable-information-pii-compromise-of-nasa-servers/ (25/02/2023).
516. Gates D. (2018) Boeing Hit by WannaCry Virus, but Says Attack Caused Little Damage. https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/ (25/02/2023).

517. AIRLIVE (2019) Alert: Over 400 Flights canceled in the U.S. due to ADS-B navigation system issue. https://airlive.net/alert-over-400-flights-canceled-in-the-u-s-due-to-ads-b-navigation-system-issue/#google_vignette (23/02/2023).
518. Solomon S. (2019) Israeli Airports Fend Off 3 Million Attempted Attacks a Day, Cyber Head Says. https://www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (23/02/2023).
519. Duvelleroy M. (2019) Airbus Statement on Cyber Incident. https://www.airbus.com/en/newsroom/press-releases/2019-01-airbus-statement-on-cyber-incident (23/02/2023).
520. Goud N. (2019) Ransomware Attack on Albany Airport on Christmas 2019. https://www.cybersecurity-insiders.com/ransomware-attack-on-albany-airport-on-christmas-2019/ (21/02/2023).
521. Team N. (2019) Cryptocurrency Miners Infected More than 50% of the European Airport Workstations. https://www.cyberdefensemagazine.com/cryptocurrency-miners-infected-more-than-50-of-the-european-airport-workstations/ (27/02/2023).
522. Debrin Foxcroft (2019) Customers could face long-term privacy issues after Air New Zealand data breach. Stuff. https://www.stuff.co.nz/business/114913189/customers-could-face-longterm-privacy-issues-after-air-new-zealand-data-breach (19/03/2023)
523. Montalbano E. (2020) DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla. https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/ (21/02/2023).
524. Dobberstein L. (2022) Ransomware grounds some flights at Indian budget airline SpiceJet. https://www.theregister.com/2022/05/26/ransomware_attack_grounds_spicejet/ (19/02/2023).
525. Chua A. (2020) Ransomware Attack hits ST Engineering's USA Aerospace Unit. https://www.flightglobal.com/aerospace/ransomware-attack-hits-st-engineerings-usa-aerospace-unit/138722.article (19/02/2023).
526. Brazilian aerospace firm Embraer hit by cyberattack | ZDNET (03/02/2023).
527. DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla | Threatpost (03/02/2023).
528. Airplane Hack Exposes Weaknesses of Alert and Avoidance Systems | Threatpost (03/02/2023).
529. Claburn, T. (2021) Airline Software Super-Bug: Flight Loads Miscalculated Because Women Using 'Miss' Were Treated as Children. https://www.theregister.com/2021/04/08/tui_software_mistake/ (25/02/2023).
530. https://www.theregister.com/2021/08/31/bangkok_airways_hit_by_lockbit/ (25/02/2023).
531. Aviation – Cyber Security Review (cybersecurity-review.com)
532. Ransomware attack grounds flights at India's SpiceJet • The Register
533. https://www.aviationtoday.com/2022/11/16/cyber-incident-impacts-boeing-subsidiary-jeppesens-flight-planning-tools/ (25/02/2023).
534. Cyber vulnerability in networks used by spacecraft, aircraft and energy generation systems | University of Michigan News (umich.edu) (01/03/2023).
535. Did Russian hackers take down U.S. airport websites? (usatoday.com) (01/03/2023).
536. Lazarus hackers abuse Dell driver bug using new FudModule rootkit (bleepingcomputer.com) (01/03/2023).

537. New Wave of Espionage Activity Targets Asian Governments | Symantec Enterprise Blogs (security.com) (01/03/2023).
538. Modem-wiping malware caused Viasat broadband outage • The Register (01/03/2023).
539. Powerful cyber attack on Russia's Civil Aviation Authority servers: no more data nor back-up - Aviation24.be (01/03/2023).
540. Hacker finds copy of TSA no-fly list on exposed cloud storage – Cyber Security Review (cybersecurity-review.com) (01/03/2023).
541. Air France and KLM notify customers of account hacks (bleepingcomputer.com)
542. https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/european-international-airport-workstations-infected-with-persistent-anti-coinminer-malware (25/02/2023).
543. FDA (2008) Federal Register, 73(1), 336–381. https://www.fec.gov/resources/legal-resources/explanation-justifications/2008/notice_2007-28.pdf (25/02/2023).
544. Aero News Network. (2010) FAA Tells Boeing To "Hack Proof" 747-8, -8F. http://www.aero-news.net/index.cfm?do=main.textpost&id=c54094a8-d6cd-404f-82d6-5598267eea23 (21/02/2023.).
545. Zimmerman M. (2015) Security expert pulled off flight by FBI after exposing airline tech vulnerabilities. Fox News. https://www.foxnews.com/us/security-expert-pulled-off-flight-by-fbi-after-exposing-airline-tech-vulnerabilities (25/02/2023).
546. Moran N., De Vynck G. (2015) WestJet Hijack Signal Called False Alarm. Bloomberg. https://www.bloomberg.com/news/articles/2015-01-10/westjet-hijack-signal-called-false-alarm#xj4y7vzkg (20/02/2023).
547. https://www.darkreading.com/iot/threat-of-a-remote-cyberattack-on-today-s-aircraft-is-real (25/02/2023).
548. Cusick S.K., Cortés A.I., Rodrigues C.C. (2017) Commercial aviation safety. 6th ed., McGaw Hill Education.
549. Airports and nuclear power stations on terror alert as government officials warn of 'credible' cyber threat – Cyber Security Review (cybersecurity-review.com) (20/02/2023).
550. 'Significant amount' of sensitive security data stolen in Perth Airport hacking | The West Australian ((10/02/2023).
551. Fury of families stranded at Heathrow after British Airways cancelled all short-haul flights | Daily Mail Online (15/02/2023).
552. Airport services firm Swissport reports ransomware incident | ZDNET (25/02/2023).
553. Gregersen E. Possible causes of the aircraft's disappearance. Britannica. https://www.britannica.com/event/Malaysia-Airlines-flight-370-disappearance/Possible-causes-of-the-aircrafts-disappearance (03/03/2023).
554. Wang. A. B. (2017) Years After Flight 370 Disappearance. The Washington Post. https://www.washingtonpost.com/news/innovations/wp/2017/04/20/years-after-flight-370-disappearance-malaysia-airlines-agrees-to-track-its-planes-from-space/ (03/03/2023)
555. Missing Malaysia plane MH370: What we know? https://www.bbc.com/news/world-asia-26503141 (25/02/2023).
556. https://www.britannica.com/event/Malaysia-Airlines-flight-370-disappearance/Possible-causes-of-the-aircrafts-disappearance (01/03/2023).

557. Denayer S. (2017) ″Search for Malaysia Airlines Flight 370 finally called off with mystery unsolved″. The Washington Post. https://www.washingtonpost.com/world/search-for-malaysia-airlines-mh370-finally-called-off-with-mystery-unsolved/2017/01/17/3662d778-dc84-11e6-ad42-f3375f271c9c_story.html (03/03/2023)
558. https://www.infrastructure.gov.au/infrastructure-transport-vehicles/aviation/aviation-safety/aviation-accident-investigations/joint-agency-coordination-centre (03/03/2023).
559. Wootson Jr.C.R. (2018) H370 experts think they've finally solved the mystery of the doomed Malaysia Airlines flight. The Washington Post. https://www.seattletimes.com/nation-world/mh370-experts-think-theyve-finally-solved-the-mystery-of-the-doomed-malaysia-airlines-flight (03/03/2023).
560. Sinha S. (2015) A History of Crashes Caused by Pilots' Intentional Acts. The New York Times. https://www.nytimes.com/interactive/2015/03/26/world/history-plane-crashes-pilots.html (03/03/2023).
561. Kylie N. (2022) Disputed Causes: The Mystery Of SilkAir Flight 185. Simple Flying. https://simpleflying.com/silkair-flight-185-mystery/ (03/03/2023).
562. BBC News (2017) Germanwings crash: Who was co-pilot Andreas Lubitz? https://www.bbc.com/news/world-europe-32072220 (03/03/2023).
563. Avionics International. An Operators An Operator's Guide to Flight Tracking Solutions https://interactive.aviationtoday.com/avionicsmagazine/december-2016-january-2017/an-operators-guide-to-flight-tracking-solutions (03/03/2023).
564. BBC News (2019) Boeing 737 Max: What went wrong? https://www.bbc.com/news/world-africa-47553174 (03/03/2023)
565. https://www.fss.aero/accident-reports/dvdfiles/ET/1996-11-23-ET.pdf (03/03/2023).
566. https://www.oig.dot.gov/sites/default/files/Audit%20Annoucement%20-%20FAA%27s%20Oversight%20of%20the%20Boeing%20737%20MAX%20Certification.pdf (03/03/2023).
567. FlightGlobal. https://www.flightglobal.com/news/articles/dot-launches-committee-to-review-faa-aircraft-certif-456889/ (05/03/2023)
568. https://www.aerotime.aero/articles/22788-more-than-400-pilots-of-737-max-are-suing-boeing-for-cover-up (01/03/2023).
569. Boeing, 737 MAX Updates. https://www.boeing.com/commercial/737max/737-max-software-updates.page (25/02/2023).
570. https://techxplore.com/news/2019-08-boeing-ceo-max-year.html (01/03/2023).
571. Reuters, China moving 'step by step' in recertifying Boeing 737 MAX. https://www.reuters.com/business/aerospace-defense/china-moving-step-by-step-recertifying-boeing-737-max-2021-03-01/ (01/02/2023).
572. Gates D., Baker M. (2019) The inside story of MCAS: How Boeing's 737 MAX system gained power and lost safeguards. The Seattle Times. https://www.seattletimes.com/seattle-news/times-watchdog/the-inside-story-of-mcas-how-boeings-737-max-system-gained-power-and-lost-safeguards/ (03/03/2023).
573. Godlewski M. (2022) NTSB: ADS-B Shows Unstabilized Approach for Learjet in El Cajon Accident. FLYING. https://www.flyingmag.com/ntsb-ads-b-shows-unstabilized-approach-for-learjet-in-el-cajon-accident/ (03/03/2023).
574. Godlewski M. (2022) NTSB Releases Preliminary Report on Fatal Texas Midair Collision. FLYING. https://www.flyingmag.com/ntsb-releases-preliminary-report-on-fatal-texas-midair-collision/ (03/03/2023).

575. Civil Aviation Administration of China (2022) Preliminary Findings on China Eastern Plane Crash Released. CAAC News. http://www.caac.gov.cn/en/XWZX/202204/t20220426_213009.html (03/03/2023).
576. Scarr S., Kawoosa V.M., Sharma M. (2022) The plunge from 29,000 feet. How China Eastern Airlines flight MU5735 went from an uneventful flight at cruising altitude to disaster in just minutes. FlightRadar24. https://graphics.reuters.com/CHINA-CRASH/ANALYSIS/movanbqyxpa/ (03/03/2023).
577. AirNav Radarbox (2022) China eastern airlines carrying 132 people crashes in China. Radarbox blog. https://www.radarbox.com/blog/china-eastern-airlines-boeing-737-carrying-132-people-crashes-in-china (03/03/2023).
578. Petchenik I. (2022) Using the New Flightradar24 KML and CSV Export Tools. Flightradar24. https://www.flightradar24.com/blog/using-the-new-flightradar24-kml-and-csv-export-tools/ (03/03/2023).
579. Petchenik I. (2023) United Airlines 777 dives after departure. Flightradar24. https://www.flightradar24.com/blog/united-airlines-777-dives-after-departure/ (03/03/2023).
580. Bajović M., Živanović M., Rašuo B., Stojaković P. (2010) New General Approach to Airplane Rotation Analysis. Trans. Jpn. Soc. Aeronaut. Space Sci., 53(180), 130–137. https://doi.org/10.2322/tjsass.53.130.
581. Stojaković P., Rašuo B. (2016) Minimal safe speed of the asymmetrically loaded combat airplane, Airc. Eng. Aerosp. Technol., 88(1), 42–52. DOI 10.1108/AEAT-03-2014-0033.
582. Stojaković P., Rašuo B. (2016) Single propeller airplane minimal flight speed based upon the lateral maneuver condition. Aerosp. Sci. Technol., 49, 239–249. doi: 10.1016/j.ast.2015.12.012.
583. Stojaković P., Velimirović K., Rašuo B. (2018) Power optimization of a single propeller airplane take-off run on the basis of lateral maneuver limitations. Aerosp. Sci. Technol., 72, 553–563, doi: 10.1016/j.ast.2017.10.015.
584. Petchenik I. (2023) Qatar Airways flight 787 loses height after take off. Flightradar24. https://www.flightradar24.com/blog/qatar-airways-flight-787-loses-height-after-take-off/ (03/03/2023).
585. Flightradar24. https://www.flightradar24.com/blog/united-airlines-777-dives-after-departure/ (03/03/2023).
586. Saračević M., Adamović S., Maček N., Aybeyan S., Pepić S. (2021) Source and channel models for secret-key agreement based on catalan numbers and the lattice path combinatorial approach. J. Inf. Sci. Eng., 37(2), 469–482. DOI: 10.6688/JISE.202103_37(2).0012.
587. Saračević M., Adamović S., Maček N., Elhoseny M., Sarhan S. (2020) Cryptographic keys exchange model for smart city applications. IET Intell. Transp. Syst., 14(11), 1456–1464. doi: 10.1049/iet-its.2019.0855.
588. Saračević M., Adamović S., Miškovic V., Elhoseny M., Maček N., Selim M.M., Shankar K. (2021) Data encryption for internet of things applications based on catalan objects and two combinatorial structures“. IEEE Trans. Reliab., 70(2), 819–830. doi: 10.1109/TR.2020.3010973.
589. EASA (2023) Safety Information Bulletin (SIB No 2022-02R1, Issued 17/02/2023).
590. ICAO (2019) Working Paper. Assembly–40th session (technical commission). A40-WP/460. Agenda Item 28: Aviation Safety and Air Navigation Policy – The application and benefits of space-based ADS-B data in the development of safety

performance indicators in support of ICAO's data-driven approach to enhancing global aviation safety.
https://www.icao.int/Meetings/a40/Documents/WP/wp_460_en.pdf (15/03/2023).

БИОГРАФИЈА АУТОРА

Дејан Кожовић, основно образовање, као и средњу школу – Десету београдску гимназију, завршио је у Београду. Звање професионални пилота, стекао је 1998. године, након успешног завршетка Пилотске академије – JAT у Вршцу. Такође, звање машински инжењер – пилот стекао је 2000. године на Вишој машинској школи ″Нада Димић″ у Земуну. Основне академске студије (студијски програм – Аеронаутика) завршио је на Факултету за цивилно ваздухопловство, Мегатренд универзитета, 2018. године, где је завршио и мастер академске студије 2019. године (студијски програм – Безбедност у ваздухопловству). Докторске студије уписао је академске 2019/20 на Факултету за компјутерске науке, Мегатренд универзитета у Београду. Све испите и друге обавезе предвиђене наставним планом и програмом ових докторских студија успешно је завршио академске 2020/2021. године. Аутор је неколико научно-истраживачких радова објављених у научним часописима са рецензијом. Течно говори енглески језик (Language proficency english level 6), као и поседује основно знање италијанског језика. Обавља послове професионалног пилота у саобраћају од 2000. године, за шта је квалификацију стекао на Пилотској академији – JAT у Вршцу (1998. године), као и у Flight Safety International у Вичити (САД), 2008. године.

СПИСАК ОБЈАВЉЕНИХ РАДОВА

1. Kožović D., Đurđević D. (2019) Sajber bezbednost u avijaciji. Megatrend revija, 16(2), 39–56.

   doi:10.5937/MegRev1902039K.

2. Kožović D., Đurđević D. (2021) Spoofing in aviation: security threats on GPS and ADS-B systems. Vojnotehnički glasnik/Mil. Tech. Cour., 69(2), 461–485.

   http://www.vtg.mod.gov.rs/archive/2021/military-technical-courier-2-2021.pdf

3. Kožović D., Đurđević D. (2021) Spufing u civilnoj avijaciji: bezbednost i sigurnost GPS/GNSS i ADS-B Sistema. Megatrend revija, 18(3), 281–306. doi:10.5937/MegRev2103281K.

4. Dinulović M., Trninić M., Rašuo B., Kožović D. (2023) Methodology for

   aeroacoustic noise analysis of 3-Bladed H-Darrieus wind turbine. Therm. Sci., 27(1A), 61–69.

   doi:10.2298/TSCI2301061D.

5. Kožović V. D., Đurđević Ž. D., Dinulović R. M., Milić S., Rašuo P. B. (2023) Air

   Traffic Modernization and Control: ADS-B System Implementation Update 2022 – a Review. FME Trans., 51(1), 117–130.

   https://www.mas.bg.ac.rs/_media/istrazivanje/fme/vol51/1/13_kozovic_at_al.pdf

Прилог 1.

Изјава о ауторству

Име и презиме аутора Дејан Кожовић_____

Број индекса 520001/2019_____

Изјављујем

да је докторска дисертација под насловом

Мултидисциплинарни аспекти сајбер безбедности авио система ADS-B

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, _25.03.2023._____

_____

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора __Дејан Кожовић_____

Број индекса _____520001/2019_____

Студијски програм _____

Наслов рада _Мултидисциплинарни аспекти сајбер безбедности авио система ADS-B

Ментор _____проф. др Немања Мачек_____

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, _25. 03. 2023._____

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Мултидисциплинарни аспекти сајбер безбедности авио система ADS-B

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, __25. 03. 2023_____

Прилог 4.

smatsa

Служба за калибражу
CAL.00_____
20.02.2023. године

ПОТВРДА

Одобрава се Дејану (Владимир) Кожовићу коришћење ADS-B података у научно-истраживачке сврхе и израду докторске дисертације, под називом: Мултидисциплинарни аспекти сајбер безбедности авио система ADS-B.

Начелник

Иван Поповић

Контрола летења Србије и Црне Горе SMATSA доо Београд
Трг Николе Пашића 10, 11000 Београд, Република Србија, п.ф. 640, www.smatsa.rs, Тел: 011 321 8123, Факс: 011 324 0456,
МАТ. БРОЈ 17520407, ПИБ 103170161