SESAR Engage KTN – catalyst fund project final technical report

Project title:	Proof-of-concept: practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity ('ATM-cybersec')
Coordinator:	University of Jyvaskyla
Consortium partners:	N/A
Thematic challenge:	TC1 Vulnerabilities and global security of the CNS/ATM system
Edition date:	29 July 2021
Edition:	1.0
Dissemination level:	Public
Authors:	Andrei Costin / University of Jyvaskyla

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.

1. Abstract and executive summary

1.1 Abstract

During the last decade, cybersecurity started to increasingly become an issue because many ATM/ATC/aviation stakeholders rely on electronic systems for critical parts of their operations, including safety-critical functions in avionics and related software/firmware. This project aims at closing this gap by developing a proof-of-concept practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity. For this purpose we have developed from scratch a novel and unique end-to-end early stage (TRL3-4) platform as well as a comprehensive hardware/software testbed. With these, we have performed several hundreds of experimental iterations and developed four novel attacks while implementing altogether more than ten attacks. After pentesting more than 120 cumulative testbed configurations, we have discovered more than 40 vulnerabilities (e.g., Denial-of-Service, crashes, hangs) and a handful of logical and implementation bugs, all these posing imminent, realistic and dangerous cyber-physical threats to safe aviation/ATM/ATC. We also successfully re-purposed our platform for defensive mechanisms, such as "RSS-Distance" model for detecting fake/spoofed ADS-B messages. Our methodologies and results are thoroughly documented in three distinct research manuscripts that currently undergo academic peer-review.

1.2 Executive summary

The world of air transportation is in active process of getting a huge overhaul. This includes development, implementation and roll-out of strategic and enormous modernization programmes such as SESAR (EU) and NextGen (USA). These programmes bring digitalization, interconnectivity and latest technologies to the many components of the Communication Navigation Surveillance (CNS), Air Traffic Management (ATM), Air Traffic Control (ATC), and pursue important benefits for next-generation aviation in terms of efficiency, safety, and environment. ICAO estimated that by 2027 about US$120 billion will be spent on the transformation of air transportation systems, and that stakeholders (including service providers, regulators, airspace users, manufacturers, researchers), will face increased levels of interaction as new, modernized ATM operations are implemented. At the same time, as security issues related to the transformation of the aviation system are coming into view, they will require a closer collaboration among experts in safety and security disciplines, and the security matters should be considered in the system changes that lie ahead.

Cybersecurity was a relatively minor issue in CNS/ATM/aviation, however this aspect is changing. At the same time, though the adoption of new technology is an ongoing activity in CNS/ATM/aviation fields, the current pace and extent of new information technologies is notably increasing the risk from cyber attacks, which is due to an increasing number of factors including ever increasing complexity and connectivity of the systems and growing technology stacks. Hence, cybersecurity is an issue because many ATM/aviation stakeholders rely on electronic systems for critical parts of their operations, including safety-critical functions. As SESAR/NextGen transformations are implemented, the CNS/ATM/ATC/avionics (sub-)systems become an overly complex combination of modern and legacy (and everything in-between) technologies combined in unexpected ways – connected to

ethernet/internet links, communicating over several dozen frequencies/radio-links (1090 ModeS/ES, 978 UAT, 117-137 VDL2), using a similar amount of protocols and data-formats (ModeS, ADS-B ES, ADS-B UAT, TIS-B, ACARS, METAR) at various ISO/OSI-equivalent levels and processed by various types of devices (e.g., EFBs, cockpit/ATC displays). One of the practical approaches to assess/test cybersecurity levels (somehow "orthogonal" to the standard yet somewhat theoretical risk-management/risk-mitigation approach) is to actively (pen)test all the possible system instances/configurations with as many as possible pentesting inputs and scenarios. However, to the best of our knowledge there are no publicly available solutions/platforms/devices that would allow a great flexibility of (pen)testing for such a varied number of technologies/links/protocols, and importantly – provide all this at an affordable price for the final stakeholders and researchers.

This project aims at closing this gap by developing a proof-of-concept practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity. For this purpose we have developed from scratch a novel and unique end-to-end early stage (TRL3-4) platform as well as a comprehensive hardware/software testbed. With these, we have performed several hundreds of experimental iterations and developed 4 novel attacks ("ADS-B-level DoS attack", "ADS-B coordinated attackers contradictory information injection") while implementing altogether more than 10 attacks. After pentesting more than 120 cumulative testbed configurations, we have discovered more than 40 vulnerabilities (e.g., Denial-of-Service, crashes, hangs) and a handful of logical and implementation bugs, all these posing imminent, realistic and dangerous cyber-physical threats to safe aviation/ATM/ATC. At the same time and using the same platform, we implemented and evaluated several defensive approaches (such as "RSS-Distance" model and "Doppler shift effect" model) for detecting fake/spoofed ADS-B messages from attackers. We describe our methodologies and results in three distinct research manuscripts that undergo academic peer-review.

2. Overview of catalyst project

2.1 Operational/technical context

Cybersecurity was a relatively minor issue in CNS/ATM/aviation, however this aspect is changing. At the same time, though the adoption of new technology is an ongoing activity in CNS/ATM/aviation fields, the current pace and extent of new information technologies is notably increasing the risk from cyber attacks, which is due to an increasing number of factors including ever increasing complexity and connectivity of the systems and growing technology stacks. Hence, cybersecurity is an issue because many ATM/aviation stakeholders rely on electronic systems for critical parts of their operations, including safety-critical functions. As SESAR/NextGen transformations are implemented, the CNS/ATM/ATC/avionics (sub-)systems become an overly complex combination of modern and legacy (and everything in-between) technologies combined in unexpected ways – connected to ethernet/internet links, communicating over several dozen frequencies/radio-links (1090 ModeS/ES, 978 UAT, 117-137 VDL2), using a similar amount of protocols and data-formats (ModeS, ADS-B ES, ADS-B UAT, TIS-B, ACARS, METAR) at various ISO/OSI-equivalent levels and processed by various types of devices (e.g., EFBs, cockpit/ATC displays). One of the practical approaches to assess/test cybersecurity levels (somehow "orthogonal" to the standard yet somewhat theoretical risk-management/risk-mitigation approach) is to actively (pen)test all the possible system instances/configurations with as many as possible pentesting inputs and scenarios. However, to the best of our knowledge there are no publicly available solutions/platforms/devices that would allow a great flexibility of (pen)testing for such a varied number of technologies/links/protocols, and importantly – provide all this at an affordable price for the final stakeholders and researchers. This project aims at closing this gap by developing a proof-of-concept practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity.

While the main goal of the project is to architecture/design/implement a **practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity** without a particular "hard-coded" in the platform, it is important that our project demonstrates its practical application. The purpose of these pentesting scenarios is to present a starting point to extend the platform to other scenarios/protocols. In order to achieve this, we aim to implement some pentesting scenarios for ADS-B, and there are multiple reasons to why we chose ADS-B as demo pentest implementation. First, the applicant/PI is a recognized international expert in practical attacks on ADS-B protocol. Second, ADS-B is one of the cornerstone protocols of the SESAR/NextGen implementations. Last but not least, it is one of the most well-publicized protocols within SESAR/NextGen implementations with large/heterogeneous/accessible device base, and big communities of hobbyists/hackers contributing one way or another to hardware, software and security knowledge-base.

- Pentest scenarios related to **"ATM operational level ADS-B"**, i.e., aiming for red-team/purple-team/blue-team types of exercises, one aim being to test the humans in the ATM loop (e.g., CERT personnel, traffic controllers, pilots), including **Threat Image Projection** technique pretty much similar to ones used to train/test X-Ray operators in the airports. This is due to the fact that in many cybersecurity threat models, the humans are many times the weakest links in the loop, therefore require constant testing and training.

- Pentest scenarios related to **"data-communication protocol level ADS-B" and "software/hardware implementation levels of ADS-B"**, i.e., provide the ability to test at the general implementation and data-handling levels various implementations (software and hardware) of the ADS-B protocols and its extensions, regardless of the vendor (including commercial, closed-source, and open-source) and frequency (ADS-B 1090 ES, ADS-B 978 UAT), this in turn allowing to potentially find early-on both functional and security bugs.
- Pentest scenarios related to **"validation of defense/mitigation levels of ADS-B"**, i.e., provide the ability to independently and with low-cost to test in practice the effectiveness and efficiency of defense/mitigations techniques for ADS-B (e.g., integrity-checks, crypto-extensions) such as the ones implemented by "Engage KTN - Authentication and integrity for ADS-B".

2.2 Project scope and objectives

The core goals and objectives of this project are as follows:

- *Goal 1 (main)*: Architecture/design a **practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity**
- *Goal 2*: Develop and demonstrate a full-blown **prototype with increased TRL** (TRL3-4)
- *Goal 3*: **Develop and validate well-documented penetration testing methodology/checklists for ATM/avionics cybersecurity** that could serve in the future as blueprints:
  a) cybersecurity guidelines/standards focused on the ATM/avionics vertical as well as
  b) catalysts for value-added services within the cybersecurity solutions/services space
- *Goal 4*: Develop and demonstrate the practical pentesting applications of our platform, using several ADS-B scenarios as starting point.

All goals have been achieved at the end of the project.

2.3 Research carried out

In summary, during this project we have built two major parts: the pentesting platform itself (the TE - a combination of own software modules and a wide-range of supported SDRs) and the testbed platform (a wide range of tested configurations DUT/SUT).

More specifically, the main research carried our and the results of each paper are presented below:

- *"Practical denial-of-service and combined high-level attacks on real-world ADS-B, ATC, ATM hardware and software."* [2]
  - In this work, we explore the cybersecurity posture of multiple ADS-B solutions (both 1090ES and UAT978) when facing high-level Denial-of-Service (DoS) or combined attacks, and we perform this by developing a platform for cybersecurity pentesting of ADS-B and adjacent systems. For example, we show that: many mobile cockpit and Electronic Flight Bag (EFB) setups can be quickly and easily crashed by remote DoS attacks; novel coordinated ADS-B attacks expose logical vulnerabilities in ADS-B systems; and the DoS attack on ADS-B IN can (dangerously) impact the performance of ADS-B OUT. Altogether

we have tested 68 different ADS-B configurations (mobile and non-mobile) for ADS-B IN DoS attack. We managed to crash 25% of them mostly within 2 minutes, while overall the DoS attack impacted 51.47% of tested configurations.

- *"Cybersecurity attacks against software logic and error handling within ADS-B implementations: systematic testing of resilience, and implementation of some countermeasures."* [3]
    - Overall, in a controlled environment we have implemented and tested 12 attacks on ADS-B, out of which **4 represent our novel contributions** to the field of ADS-B security. For all these attacks we developed a unique testbed consisting of 12 hardware devices and 20 software (Android, iOS, Linux, Windows) **resulting in a total of 34 tested configurations. Worryingly, each of the attacks were successful on various subsets of the tested configurations. In some attacks, we discovered wide qualitative variations and discrepancies on how particular configurations react to and treat ADS-B inputs that contain errors or contradicting flight information, with the main culprit almost always being the software implementation.**
- *"Fuzzing 'GDL-90 Data Interface Specification' within aviation software and avionics devices – a cybersecurity perspective."* [4]
    - We captured legitimate traffic from ADS-B avionics devices and repurposed the captures to our fuzzing scenarios. We ran our samples through a state-of-the-art fuzzing platform (AFL), and fed the output AFL's to the EFB apps and GDL-90 decoding software via the network in the same manner as legitimate GDL-90 traffic is sent from ADS-B and other avionics devices. The result shows a worrying lack of security in many EFB applications where the security is directly related to aircraft's safety navigation. **Out of 16 tested configurations, our avionics pentesting platform managed to crash or otherwise impact 9 (or 56%) of those.** The observed problems manifested as crashes, hangs, and abnormal behaviours of the EFB apps and GDL-90 decoders during the fuzzing test.

We used state-of-the-art approaches to devise sound methodologies, and below we present the high-level architectural views of our approaches:

Approach from "Cybersecurity attacks against software logic and error handling within ADS-B implementations: systematic testing of resilience, and implementation of some countermeasures." [3]:

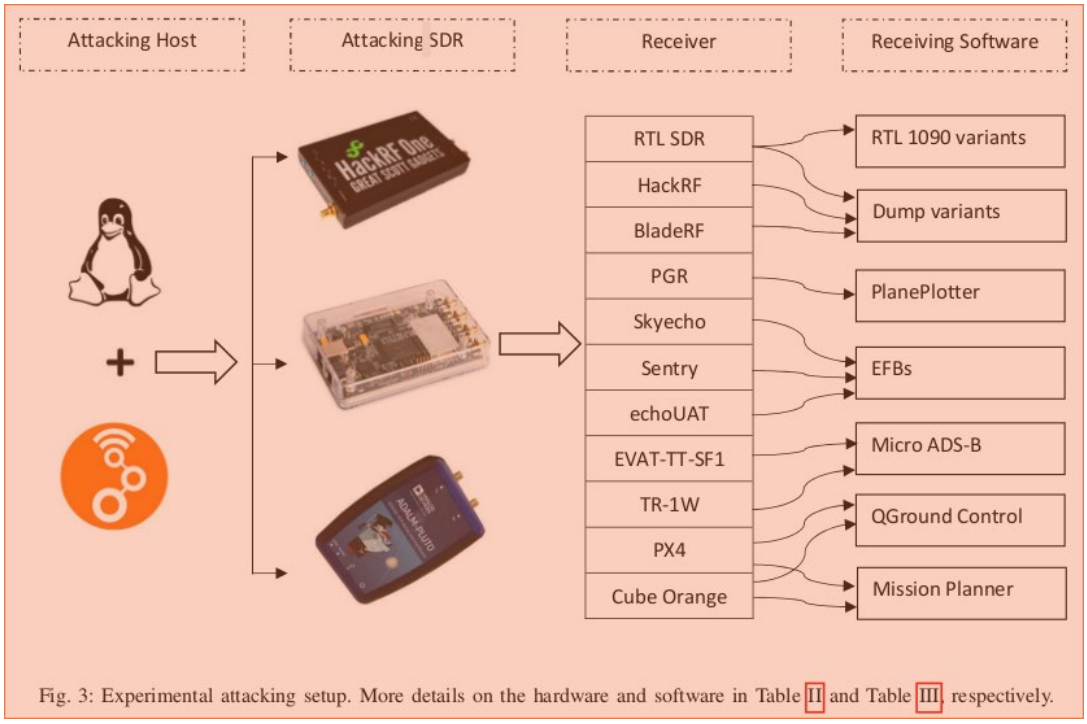
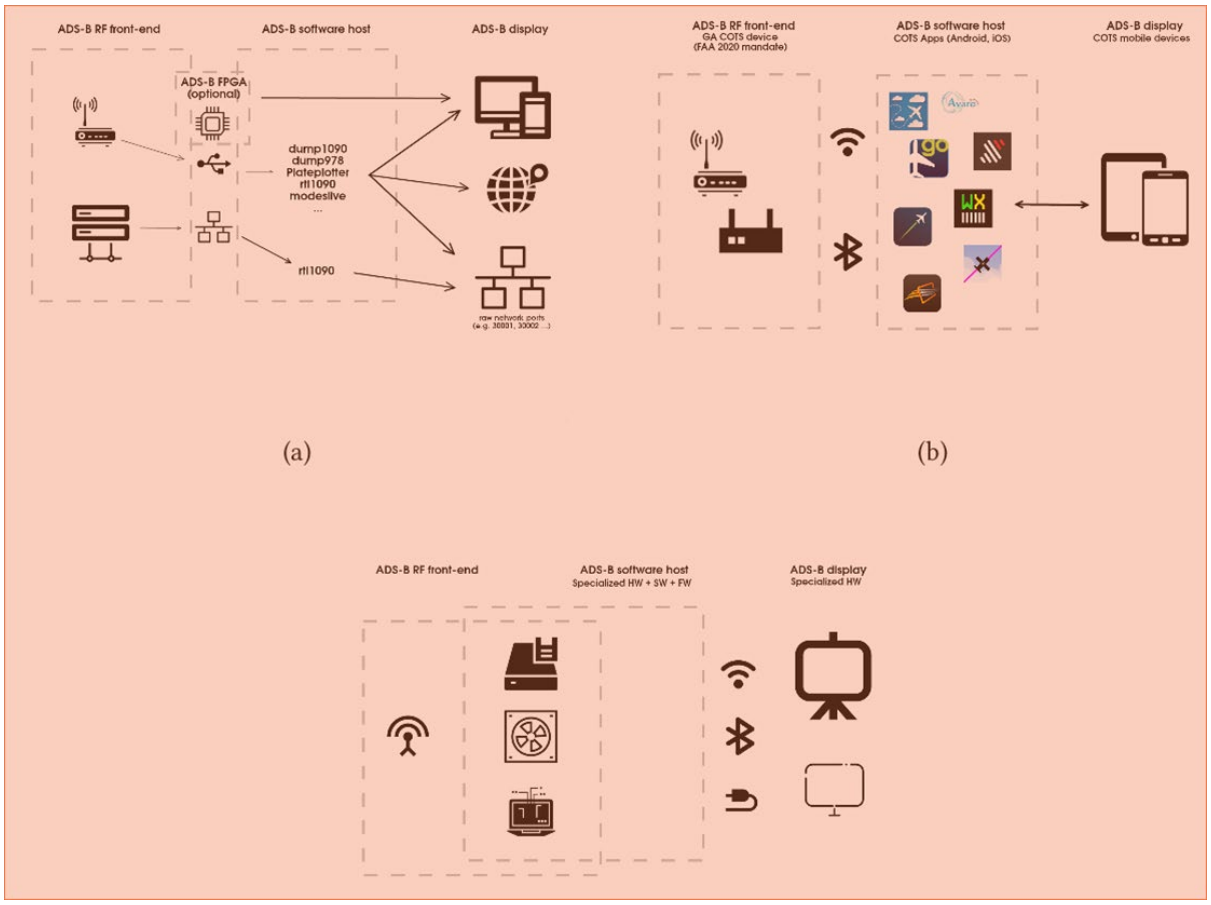
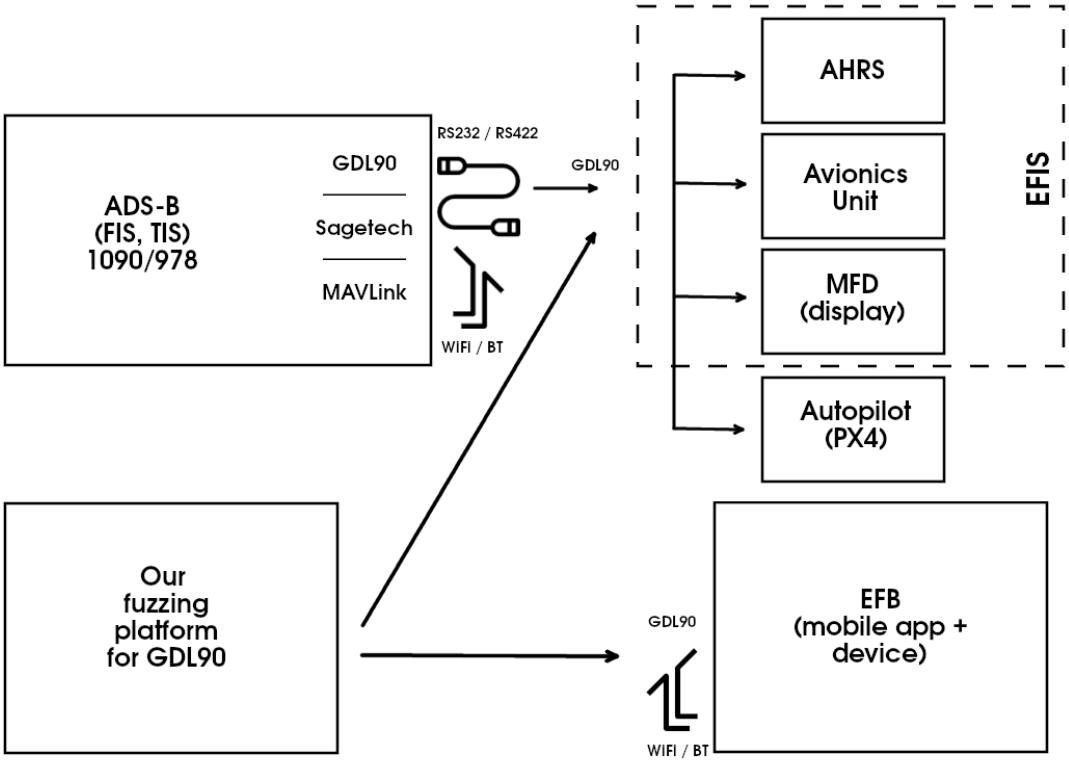


Fig. 3: Experimental attacking setup. More details on the hardware and software in Table II and Table III, respectively.

Approach from "Practical denial-of-service and combined high-level attacks on real-world ADS-B, ATC, ATM hardware and software." [2]:



Approach from “Fuzzing 'GDL-90 Data Interface Specification' within aviation software and avionics devices – a cybersecurity perspective.” [4]:



2.4 Results

From scientific point of view, the main results are as follows:

- Preparation and submission for peer-review of three (3) high-quality research papers [2] [3] [4] (Section).
- Development of systematic methodologies for cybersecurity assessment and pentesting that are specific to avionics/aviation/ATM/ATC fields, in particular to ADS-B and GDL-90 implementations whether in hardware or in software.
- Discovery of several dozen serious vulnerabilities (e.g., crashes, hangs, wrong position calculations) in a large set of software/hardware configurations.

More specifically, the main results of each paper are presented below:

- *“Practical denial-of-service and combined high-level attacks on real-world ADS-B, ATC, ATM hardware and software.”* [2]

- **Tested 68 different ADS-B configurations (mobile and non-mobile) for ADS-B IN DoS attack. We managed to crash 25% of them mostly within 2 minutes, while overall the DoS attack impacted 51.47% of tested configurations.**

- *"Cybersecurity attacks against software logic and error handling within ADS-B implementations: systematic testing of resilience, and implementation of some countermeasures."* [3]
  - **A total of 34 tested configurations. Worryingly, each of the attacks were successful on various subsets of the tested configurations. In some attacks, we discovered wide qualitative variations and discrepancies on how particular configurations react to and treat ADS-B inputs that contain errors or contradicting flight information, with the main culprit almost always being the software implementation.**
- *"Fuzzing 'GDL-90 Data Interface Specification' within aviation software and avionics devices – a cybersecurity perspective."* [4]
  - **Out of 16 tested configurations, our avionics pentesting platform managed to crash or otherwise impact 9 (or 56%) of those.** The observed problems manifested as crashes, hangs, and abnormal behaviours of the EFB apps and GDL-90 decoders during the fuzzing test.

3. Conclusions, next steps and lessons learned

3.1 Conclusions

- Our final main result is a pentesting platform having a relatively high TRL level (TRL3-4), therefore it represent a good and mature starting point to increase the cybersecurity of aviation/ATM/ATC in a practical and effective manner.
- The practical demonstration that major combinations of software+hardware can be remotely impacted (e.g., crashed, potential remote code execution) with a relative ease and modest budget is worrying and should be a strong driving force for the impacted/relevant stakeholders to accelerate the cybersecurity improvements by employing our expertise and platform, or by building atop our methods.
- The consistency of our results on a very broad range of hardware-software configurations indicate the reliability of our proposed methodology as well as the effectiveness and efficiency of our platform. We hope our platform, results and reported vulnerabilities can help improve the overall cybersecurity posture of ADS-B software, firmware, and hardware.
- We believe that not enough testing and certification is performed on many recent ADS-B solutions on the market. Because of the ADS-B mandates, the necessity of having ADS-B solutions on-board have created high-demand therefore many solutions (both hardware, software, hardware + software) flooded the market. However, a large part of solutions do not have adequate cybersecurity assessment/testing/quality. This is further fuelled by the fact that mobile ADS-B software (e.g., apps, EFBs) are in a gray area of “certification” and hence do not undergo the same regulatory and certification procedures as the classical avionics all-in-one systems.
- We urge the impacted/relevant stakeholders to contact us for immediate research and industry collaborations as cybersecurity the presented cybersecurity risks/attacks are very real and imminent.

3.2 Next steps

- Project results will be presented at official Engage TC1 “Vulnerabilities and global security of the CNS/ATM system” workshop in Sep 2021 (organized by Innaxis).
- Project results are expected to be presented at SESAR Innovation Days 2021 (e.g., poster, summary paper).
- Project results are expected to be presented at top international cyberscurity industry conferences (e.g., BlackHat, RSA Conference, etc.).
- Seeking future funding calls (e.g., SESAR, Catalyst, NGI) for R&D&I to further mature the technology and achieve more novel results and insights both from academic/research as well as industry perspectives.
- Plan and investigate tech-transfer options so that the technology can be effectively and efficiently applied within industry.

3.3 Lessons learned

- The timing of this project and its funding size is very appropriate.
- Despite COVID19 uncertainty, we believe we managed the project quite well given the circumstances (e.g., equipment orders&shipping affected delaying some experiments, etc.).
- We believe “light touch” catalyst funding approach works very well – as researchers, we encourage more such initiatives in general, as it cuts the unnecessary overheads and leave enough room for researchers to focus on the actual research.
- We also support the idea of “similar sized” budgets to be available for potential future KTN and other calls.
- The quality and the size of the mentor groups were very-very good in our case, the periodicity of the mentor calls was adequate.

4. Dissemination

The project's page in JYU's official projects repository is publicly accessible at [1]. During the project execution, the main dissemination activities revolved around peer-reviewed paper publications [2] [3] [4]. Some project highlights have been disseminated during a JYU cybersecurity webinar (~100 attendees) [5] [6]. Project results will be further disseminated at official Engage TC1 "Vulnerabilities and global security of the CNS/ATM system" workshop in Sep 2021 (organized by Innaxis).

5. References

5.1 Project outputs

1. Official Project entry in JYU grants/funding/projects system Converis: https://converis.jyu.fi/converis/portal/detail/Project/36260337?auxfun=&lang=fi_FI
2. Peer-review publication: *"Practical denial-of-service and combined high-level attacks on real-world ADS-B, ATC, ATM hardware and software."*, Syed Khandker, Hannu Turtiainen, Andrei Costin (Under review, submitted to ACM Transactions on Privacy and Security (TOPS))
3. Peer-review publication: *"Cybersecurity attacks against software logic and error handling within ADS-B implementations: systematic testing of resilience, and implementation of some countermeasures."*, Syed Khandker, Hannu Turtiainen, Andrei Costin, Timo Hämäläinen, (Under review, submitted to IEEE Transactions on Aerospace and Electronic Systems (TAES))
4. Peer-review publication: *"Fuzzing 'GDL-90 Data Interface Specification' within aviation software and avionics devices – a cybersecurity perspective."*, Hannu Turtiainen, Syed Khandker, Andrei Costin, Timo Hämäläinen, (Under review, submitted to IEEE Transactions on Aerospace and Electronic Systems (TAES))
5. JYU Online Webinar "Kybermaailma - uhka vai mahdollisuus" ("The cyber world - a threat or an opportunity") https://www.jyu.fi/fi/ajankohtaista/arkisto/2021/06/kybermaailma-uhka-vai-mahdollisuus-webinaarin-esitykset
6. Announcement the JYU Online Webinar "Kybermaailma - uhka vai mahdollisuus" ("The cyber world - a threat or an opportunity") https://www.sttinfo.fi/tiedote/kutsu-medialle-kybermaailma---uhka-vai-mahdollisuus--webinaari-166-klo-9?publisherId=69817172&releaseId=69911765
7. An extensive list of security bugs/vulnerabilities to be reported via "responsible disclosure" process to the corresponding vendors.

5.2 Other

[O1] "Andrei Costin – LinkedIn", https://www.linkedin.com/in/costinandrei/
[O2] "Andrei Costin – Google Scholar Citations", https://scholar.google.fr/citations?user=QANNFaQAAAAJ&hl=en&oi=ao
[O3] ***"Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices"***, **A Costin**, A Francillon, https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf
[O4] ICAO TWELFTH AIR NAVIGATION CONFERENCE (Montréal, 19 to 30 November 2012) - CYBER SECURITY FOR CIVIL AVIATION, https://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENonly.pdf
[O5] "A Large Scale Analysis of the Security of Embedded Firmwares", **A Costin**, J Zaddach, A Francillon, D Balzarotti

[O6] “Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces”, **A Costin**, A Zarras, A Francillon
[O7] “A Dangerous 'Pyrotechnic Composition': Fireworks, Embedded Wireless and Insecurity-by-Design”, **A Costin**, A Francillon
[O8] “APPIOTS: tools for addressing vulnerabilities in software and firmware of IoT/embedded devices” https://www.jyu.fi/it/en/research/research-projects/business-finland/appiots
[O9] NIH REACH – Incubator Program, https://www.nordicinnovationhouse.com/siliconvalley/sv-programs/reach
[O10] “HORIZON 2020 –WORK PROGRAMME - G. Technology readiness levels (TRL)”, https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf
[O11] “Engage KTN - Authentication and integrity for ADS-B”, https://engagektn.com/wp-content/uploads/2019/12/C3-Authentication-integrity-ADS-B.pdf
[O12] “Air Traffic Security: Aircraft Classification Using ADS-B Message's Phase-Pattern”, https://www.mdpi.com/2226-4310/4/4/51/pdf
[O13] “ECSO TRANSPORTATION SECTOR REPORT Cyber security for road, rail, air, and sea”, https://ecs-org.eu/documents/publications/5e78cb9869953.pdf

Annex I: Acronyms

Term	Definition
ADS-B	Automatic Dependent Surveillance–Broadcast
UAT	Universal Access Transceiver
FAA	Federal Aviation Administration
ATM	Air Traffic Management
ATC	Air Traffic Control
UAV	Unmanned Aerial Vehicle
UAS	Unmanned Aircraft Systems
GDL-90	Garmin Data Link protocol
TE	Testing Equipment
DUT	Device Under Test
SUT	Software Under Test