Securing the Digital Sky: a scenario-driven study on the enhancement of cybersecurity in location-independent aerodrome control systems

Gabor Horvath
Ludovika University of Public Service
Doctoral School of Military Engineering
Budapest, Hungary
0000-0002-2939-1426

***Abstract* — The rapid advancement of technology in aviation business management, notably through the implementation of location-independent aerodrome control systems, is reshaping service efficiency and cost-effectiveness. However, this emphasis on operational enhancements has resulted in a notable gap in cybersecurity incident management proficiency. This study addresses the escalating sophistication of the cybersecurity threat landscape, where malicious actors target critical safety information, posing risks from disruptions to potential catastrophic incidents. The paper employs a specialized conceptualization technique, derived from prior research, to analyze the interplays between malicious software and degraded modes operations in location-independent aerodrome control systems. Rather than predicting attack trajectories, this approach prioritizes the development of training paradigms to rigorously evaluate expertise across engineering, operational, and administrative levels in air traffic management domain. This strategy offers a proactive framework to safeguard critical infrastructures, ensuring uninterrupted, reliable services, and fortifying resilience against potential threats. This methodology promises to cultivate a more secure and adept environment for aerodrome control operations, mitigating vulnerabilities associated with malicious interventions.**

Keywords—remote tower, location-independent aerodrome control, cybersecurity, air traffic management

I. INTRODUCTION

The trajectory of air traffic management has been significantly influenced by the remarkable progress in the semiconductor domain observed over recent decades. Central to this metamorphosis is Moore's Law, postulating that the computational capacity, delineated by transistor count on integrated circuits, amplifies twofold approximately every 18-24 months [1]. This exponential growth, rooted in technological miniaturization, epitomizes the essence of contemporary digital systems pivotal for the context of this paper.

Historically, key aerodromes necessitated dedicated air traffic control infrastructures, including the control tower equipped with its integrated systems, to ensure safe, orderly, and expeditious flow of air traffic. Yet, the domain of Information and Communication Technologies has experienced unprecedented advancements, heralding the inception of the location-independent aerodrome control, also known as Remote Tower Service (rTWR). This encompasses essential apparatuses for orchestrating location-independent aerodrome control services proximate to, or within, an aerodrome. Miniaturization, as previously elucidated, is instrumental in refining these apparatuses, not merely in terms of physical dimensions but also in optimizing energy efficiency and economizing production expenditures. These synergistic attributes have ushered in a transformative phase, diminishing the indispensability of conventional tower control edifices in contemporary air traffic management.

Leveraging the rTWR suite, predominantly characterized by advanced camera systems, air traffic control can now be adeptly administered from geographically distant locales, rendering this service more spatially versatile [2]. Yet, the cybersecurity vulnerabilities of location-independent aerodrome control are yet to be explored, since traditionally the term security had a physical focus in the aviation domain overall [3]. This focus has transitioned to an epoch emphasizing information security, commonly termed as cybersecurity. The contemporary cybersecurity threat matrix has grown in complexity, with adversaries ranging from those seeking to perturb safety-critical information to those harboring intentions that could culminate in tragic consequences.

To address the aforementioned challenges, the researcher developed and applied a novel conceptualization technique termed 'Scrutiny for Susceptibility and Negligence' (S2N). This methodology is designed to analyze the interplay between malicious software and degraded operational states. S2N method derives its foundation from both hypothesized [4] and established [5] attack strategies, drawing insights from prior incidents materialized and theorized impacting safety-critical systems and tactics employed across various sectors. This fosters the generation of hybrid scenarios, amalgamating diverse strategies to formulate innovative attack conjectures. Therefore, the primary objective of this study is, by using the resultant models, to facilitate collaborative sessions among multidisciplinary teams, orchestrating and authenticating cyber-exercise agendas, therefore enhancing the cybersecurity level of rTWR systems.

II. METHODOLOGY

The comprehensive literature review reveals notable research gaps, which have been officially acknowledged by prominent actors like the Single European Sky ATM Research (SESAR) program by EUROCONTROL and the USA's advanced research initiative on Air Traffic Management systems (NEXT-GEN) [6]. The methodology applied in this study was designed to tackle cybersecurity concerns within the industry [7], providing a pragmatic solution through the introduction of an unique conceptualization, delineating both 'mass produced' attacks and more intricate, sophisticated cyber

979-8-3503-7041-6/23/$31.00 ©2023 IEEE

threats targeting location-independent aerodrome control systems.

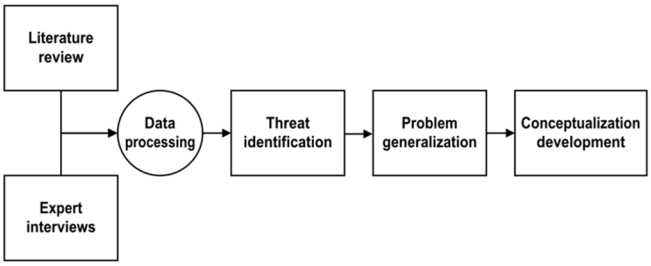

Figure 1. Applied research methodology

As Fig. 1 shows the research methodology for this study comprises a systematic five-step approach. Firstly, a comprehensive literature review was conducted, coupled with expert interviews, to establish a foundational understanding of cybersecurity threats within the aviation sector, specifically focusing on location-independent aerodrome control systems. Subsequently, the acquired qualitative data underwent its processing phase, involving organization and classification. This facilitated the identification of key patterns and recurring threat-themes laying the groundwork for a detailed examination through S2N method. Building upon this, a process of generalization was employed to extract overarching trends and patterns, providing a comprehensive understanding of the possible modus operandi of malicious actors targeting rTWR systems. This research methodology culminates in the development of two conceptual framework, which serve as the analytical tool for assessing cyber threats: (A) a comprehensive depiction of 'mass produced' attacks, emphasizing their broad reach and potential for widespread disruption, and (B) a detailed representation of sophisticated attacks, showcasing advanced tactics and their potential to impact safety-critical systems within location-independent aerodrome control.

A. Depicting 'Mass Produced' attacks

Evaluating the threats presented by malicious software (malware) remains a complex endeavor, encompassing both the likelihood of a cyber-attack and its ramifications on security. A modest yet escalating number of incidents have breached the protective barriers of Air Traffic Management structures [8] which also means that the exposure of rTWR system elements to malicious intent from cyberspace can also be prognosticated. To date, these breaches have not culminated in fatalities. One could posit those current protective measures – spanning human oversight, firewall implementations, and software-hardware diversification – offer adequate protection. Nonetheless, it's imperative to maintain vigilance, particularly in the absence of a unified perspective on impending cyber threats.

Historical cyber incursions predominantly leveraged 'mass produced' malware, not specifically targeting safety-centric infrastructures [9]. For instance, Linux.Psybot proliferated among embedded devices, notably routers equipped with Linux MIPS (Microprocessor without Interlocked Pipeline Stages) architectures. Despite its utilization of rudimentary tactics, such as brute-force authentication attacks on administrative interfaces, Psybot poses significant challenges for high-reliability platforms. Malicious software disrupts foundational assumptions regarding CPU usage, memory tasks, and network-bandwidth, which are integral to the cybersecurity triad (confidentiality, integrity, availability, CIA). Ensuring the consistent CIA of resources for a vital task becomes challenging amidst suspicions of system compromise.

Complications amplify when safety-oriented platforms are devoid of advanced network surveillance utilities. Astonishingly, many critical applications possess rudimentary tools for network traffic analysis. In certain scenarios, monitoring applications are intentionally excised post-installation, given the extensive validation and verification burdens they introduce, potentially ushering in novel failure modes.

Moreover, even with the presence of network surveillance utilities, numerous high-reliability entities are bereft of the requisite forensic expertise to ascertain the magnitude of a breach or formulate effective contingency plans. This deficiency is especially alarming for sectors obligated to uphold service standards in safety-critical contexts [10]. For instance, holding an airborne aircraft for comprehensive forensic scrutiny of a rTWR system is unfeasible. Consequently, it becomes paramount to conduct cyber-security simulations and drills, empowering service providers to counteract cyber threats while concurrently upholding operational security.

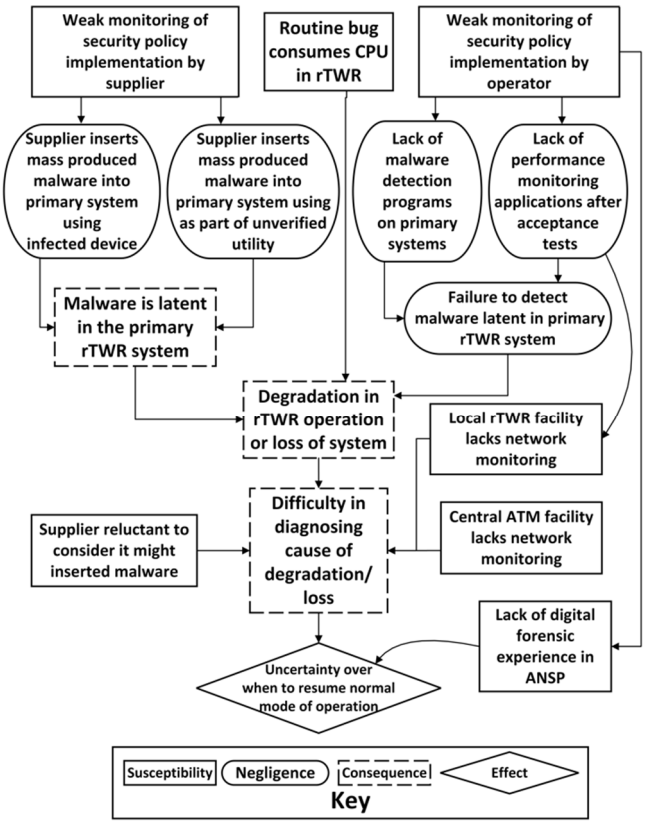

Figure 2. S2N method applied on rTWR in case of 'mass produced' malware

Fig. 2 presents the application of S2N method in modeling cyber-attack scenarios, derived from insights garnered from both hypothesized and established attack scenarios. In Fig. 2, the left upper part denotes vulnerabilities stemming from insufficient oversight of supplier adherence to an organization's security protocols. This susceptibility is linked to two distinct breaches, each correlating to different infection

methods observed in the aforementioned scenarios. The first breach involved malware introduction via a infected USB device, while the second breach occurred when malware was concealed within a module library not directly authored by the supplier, which had not undergone rigorous verification. Both attack vector possesses the potential to compromise the CIA of location-independent aerodrome control systems by malware.

Conversely, the susceptibility indicated at the right upper part of Fig. 2 pertains to managerial and organizational deficits within the ANSP, rather than external supplier issues. In one incident [11], the ANSP boasted a robust central engineering department, but malware impacted a network in a regional hub. Local engineers, despite their autonomy, lacked the resources of their national counterparts, leading to subpar network surveillance. This made it challenging to ascertain if network activity aligned with specific operational metrics, such as individual radar target packet generation. Consequently, detecting malware-induced network resource consumption became problematic. Considering this event, it becomes analytically evident that, if rTWR were implemented, the repercussions of a comparable scenario could be profound.

Another susceptibility arose from the absence of anti-malware software within primary Communication-Navigation-Surveillance (CNS) applications. The ANSP's security strategy, emphasizing a robust external defense with a less fortified internal system, was predicated on the belief that malware would never penetrate primary CNS applications. While space constraints limit the detailed exploration of this strategy within the S2N method, subsequent analyses could delve deeper.

The dearth of network surveillance tools and malware detection systems hindered malware detection in the two incidents. Immediate repercussions were absent since CNS applications are typically over-engineered to accommodate future traffic growth. However, Fig. 2 highlights a critical situation encountered by an ANSP, and consequently envisaged on rTWR, when a standard software update inadvertently introduced a glitch into a CNS application. The standard procedure of reverting to a prior system version was compromised due to inadequate documentation of pre-installation CNS system configurations. This led to a complex diagnostic process, exacerbated by the simultaneous presence of the software glitch and malware.

Fig. 2 elucidates how historical data incident can guide the preliminary phases of cyber-security training scenario creation. The complexity can be adjusted based on the exercise's intended difficulty. It is pivotal to strike a balance between overwhelming and under-challenging participants, especially in areas like forensic analysis.

The examination of past ATM incidents highlighted challenges faced by regional centers during night-shift software upgrades, particularly in securing specialist support from central engineering teams. This underscores the potential value of expanding Fig. 2 to encompass challenges faced by regional teams seeking assistance from central monitoring specialists during off-hours.

Fig. 2's concluding node emphasizes the security implications of the cyber-attack scenario. While procedural air traffic controller procedures can ensure safety during low traffic periods, prolonged system failures can still compromise safety and security levels. Decisions regarding airspace closure necessitate collaboration among engineers, managers, and operational personnel. The S2N method in Fig. 2 can be further elaborated to encompass additional effects, such as the ramifications of redirecting traffic to neighboring centers, especially if they too are malware-compromised. This scenario becomes increasingly relevant given the network integration anticipated under the application of System Wide Information Management (SWIM) components of the European ATM network.

This section delineates the interplay between standard system malfunctions, like software glitches, and prevalent malware strains, e.g., Linux.Psybot variants. While commercial anti-virus software can typically detect and contain these threats in non-critical systems, safety-related applications present a challenge. Continuous anti-virus updates are crucial, but they introduce the dilemma of ensuring these updates don't inadvertently compromise vital systems. Hence, conducting cyber-attack drills is imperative to bolster staff readiness against malware threats. This section also underscores the utility of S2N method in crafting training scenarios, aiding planning teams in ensuring an exercise's technical validity and veracity.

B. Depicting sophisticated attacks

State agency participation in malware development has arguably intensified the threat landscape, exemplified by malware strains like W32.Stuxnet, W32.Duqu, and W32.Flamer [12]. Upon the composition of this manuscript, available empirical data does not indicate any detection of these threats by ANSPs. Yet, W32.Duqu infiltrated several European safety-centric industries [13]. Consequently, cyber-security tools must adapt to evaluate the ramifications of these advanced threats on aviation domain. A notable advancement is the melding of social media with malware command and control servers. While remote host utilization for malware updates and data extraction is not novel, the proliferation of easily accessible internet services has bolstered this trend. Anonymity servers further amplify this by offering proxy services, enabling sophisticated malware to bypass previously deemed robust firewalls. For instance, Stuxnet and Duqu utilized command servers to gather data on host anti-viral measures, adjusting their strategies accordingly.

Modern malware architectures mimic the protective systems they target. They often function as loaders, modifying their attack profiles by downloading diverse definitions, thereby eluding detection. This adaptability has been evident in recent malware iterations [14]. The competency of rTWR operators, especially ANSPs, in detecting these advanced threats remains a concern. Intriguingly, malware has been identified in unconventional system components, such as graphics cards, and has leveraged diverse transmission mediums, from local networks to USB sticks. Stuxnet, for instance, capped its transmission to five new hosts, complicating traceability. The misconception that isolation from the public internet guarantees security is debunked by the transmission capabilities of these devices.

Despite stringent security protocols against portable memory devices in safety-related organizations, negligences persist. Suppliers often overlook the rationale behind these restrictions, leading to susceptibilities. Recent malware strains exhibit precision, targeting specific systems. While they may infect numerous hosts, they inflict damage selectively. This guided approach, akin to precision munitions, poses collateral

risks to rTWR systems. The inadvertent compromise of these systems, even if unintended, can have dire consequences. The potential for hostile entities to exploit these methods against safety-critical applications is real.

State machines have been innovatively integrated into malware, controlling their impact and evading detection. Stuxnet, for instance, employed a state machine to intermittently activate its malicious functions, confounding detection efforts. Such tactics pose significant challenges, especially for industries reliant on external IT service providers. The rise of Cloud architectures further complicates this landscape. State machine utilization has birthed 'land-mine' attacks, designed not to incapacitate systems but to drain engineering resources. This underscores the importance of cyber-attack drills, prompting engineers to consider malware as a potential cause of system anomalies.

Regulatory bodies play a pivotal role in cyber-security. Preliminary assessments across twenty European states indicate a glaring unpreparedness among state agencies for cyber-attacks [15]. The disconnect between safety-focused agencies and cyber-security entities exacerbates this issue. The need for collaborative efforts between these entities is ever more pressing, given the looming threat to safety-critical infrastructures. Cyber-threats are not industry specific. For instance, some European regions exhibit intertwined military and civilian air traffic management infrastructures. Testing the robustness of these defenses is paramount.

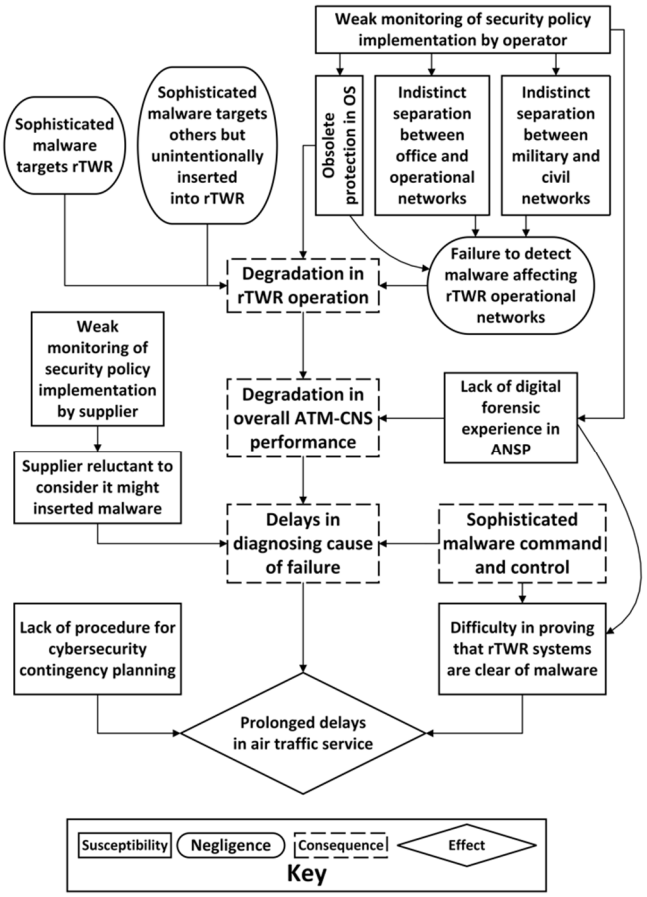

Figure 3. S2N method applied on rTWR in case of sophisticated attack

Fig. 3 offers a sophisticated cyber-attack scenario, emphasizing the indistinct separation between operational and office systems. The U.S. Department of Transport identified interdependencies in the U.S. National Air Space [16]. Fig. 3 also underscores the susceptibility of military and civil systems, focusing on deliberate network attacks, such as spurious packet broadcasting. This scenario, rooted in historical byzantine failures, introduces a state machine attack, complicating the response during a cyber-exercise. Fig. 3 poses multifaceted challenges, necessitating coordination among various stakeholders, from engineers to regulators. As with Fig. 2, the S2N method elements serve as foundational pillars for subsequent exercises, targeting a diverse stakeholder group, encompassing suppliers, engineers, managers, and regulators.

III. CONCLUSIONS

Malicious software presents an escalating threat to critical safety and security systems. The growing reliance on standardized software components renders safety-oriented systems vulnerable to widespread malware, underscoring the need for robust cybersecurity measures. This is further compounded by the emergence of advanced cyber threats, exemplified by entities like W32.Stuxnet, which require proactive mitigation strategies. The imperative to protect systems extends to a diverse cohort of professionals, including engineers, administrators, operational personnel, and regulatory bodies. Their collective efforts are pivotal in assessing potential repercussions of cyber intrusions on location-independent aerodrome control systems.

This study endeavors to comprehensively address these concerns within the domain of air traffic control scenarios. It delineates the multifaceted security implications that arise and seeks to formulate inter-agency drills for scrutinizing the expertise of stakeholders. These drills play a crucial role in ensuring seamless and secure operations. The S2N conceptualization method employed in this study offers a systematic approach to understanding and mitigating security implications. By focusing on nascent stages of scenario creation, it provides a comprehensive view of potential threats and vulnerabilities. As the aviation industry undergoes rapid digital modernization, with the adoption of automation and the enhancement of system functionalities, the need for a reliable framework for cyber resilience becomes paramount. This framework, illustrated in Fig. 2 and Fig. 3, can be applied systematically and holistically to safeguard rTWR system operations from evolving cyber threats. The significance of the issues emphasized in this study lies in the fact that previously major stakeholders have underscored the gravity of the cybersecurity aspect within the Aviation Ecosystem. Therefore, the potential benefits of the S2N method lie in the derivation of standardized regulatory frameworks and the provision of essential guidance materials conducive to a security-by-design approach.

Implementing the proposed conceptualization framework in location-independent aerodrome control systems presents a significant leap in scenario driven techniques. This framework acts as a bulwark, fortifying cyber-resilience and ensuring uninterrupted and more secure rTWR operations. By systematically identifying and mitigating potential threats, stakeholders can proactively safeguard their critical systems. Moreover, this approach promotes a culture of continuous improvement in cybersecurity practices. In prospect, forthcoming research endeavors may concentrate on the continued refinement of methodologies and frameworks to effectively address the dynamic landscape of cyber threats.

This includes harnessing advanced technologies and leveraging artificial intelligence for enhanced cybersecurity in aviation. Additionally, exploring interdisciplinary collaborations with experts in cybersecurity, artificial intelligence, and aviation engineering will be instrumental in developing innovative solutions. This research sets a precedent for the holistic integration of cybersecurity measures into the fabric of aviation ecosystem, ultimately ensuring the safety and security of air travel in an increasingly digitized world.

ACKNOWLEDGMENT

This paper was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Culture and Innovation financed from the National Research, Development and Innovation Fund.

REFERENCES

[1] E. P. DeBenedictis, “It’s Time to Redefine Moore’s Law Again”, Computer, 2017, doi: 10.1109/MC.2017.34.

[2] N. Fürstenau, Virtual and remote control tower: research, design, development and validation. New York, NY: Springer Berlin Heidelberg, 2016.

[3] G. Horváth, “The cybersecurity aspect of remote tower optical systems”, Acta Avionica, 2023, doi: 10.35116/aa.2023.0006.

[4] E. Purchase and F. Caldwell, “Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack”,Guarding Your Business, Kluwer Academic Publishers, 2004, doi: 10.1007/0-306-48638-5_4.

[5] P. Théron and S. Bologna (editors), Critical Information Infrastructure Protection and Resilience in the ICT Sector: IGI Global, 2013. doi: 10.4018/978-1-4666-2964-6.

[6] C. W. Johnson, “Cyber security and the future of safety-critical air traffic management: identifying the challenges under NextGen and SESAR”, 10th IET System Safety and Cyber-Security Conference 2015, Bristol, UK: Institution of Engineering and Technology, 2015, doi: 10.1049/cp.2015.0276.

[7] B. M. Asenahabi, Basics of Research Design: A Guide to selecting appropriate research design, 2019.

[8] B. Pancevski, “Europe’s Air-Traffic Agency Under Attack From Pro-Russian Hackers”. The Wall Street Journal, 2023.

[9] C. Johnson, “CyberSafety: CyberSecurity and Safety-Critical Software Engineering”, Achieving Systems Safety , London: Springer London, 2012, doi: 10.1007/978-1-4471-2494-8_8.

[10] X. Bellekens, R. Atkinson, A. Seeam, C. Tachtatzis, I. Andonovic, and K. Nieradzinska, “Cyber-Physical-Security Model for Safety-Critical IoT Infrastructures”, 161862 Bytes, 2016, doi: 10.6084/M9.FIGSHARE.3971523.V1.

[11] “Report Of The Irish Aviation Authority Into The ATM System Malfunction”, Irish Civilian Aviation Authority, Dublin, Ireland, 2008.

[12] A. Sharma, B. B. Gupta, A. K. Singh, és V. K. Saraswat, “Advanced Persistent Threats (APT): evolution, anatomy, attribution and countermeasures”, J Ambient Intell Human Comput, 2023, doi: 10.1007/s12652-023-04603-y.

[13] K. Hemsley és R. Fisher, “A History of Cyber Incidents and Threats Involving Industrial Control Systems”, in Critical Infrastructure Protection XII, Springer International Publishing, 2018, doi: 10.1007/978-3-030-04537-1_12.

[14] M. Guri Mordechai, Kedma Gabi, Kachlon Assaf, és Elovici Yuval, “AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies”, in 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), 2014, doi: 10.1109/MALWARE.2014.6999418.

[15] “Aviation under attack: Faced with a rising tide of cybercrime, is our industry resilient enough to cope?” EUROCONTROL, 2021

[16] “Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems (Report Number: FI-2009-049)”. Federal Aviation Administration, 2009