International Civil Aviation Organization

WORKING PAPER

AN-Conf/14-WP/173
29/7/24
(Information Paper)
English only

FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

Agenda Item 4: Hyper-connectivity of air navigation system
4.2 Cybersecurity and information system resilience

AIR TRAFFIC SAFETY ELECTRONICS PERSONNEL (ATSEP) ROLE IN CYBERSECURITY

(Presented by the International Federation of Air Traffic Safety Electronics Associations (IFATSEA))

EXECUTIVE SUMMARY

This paper presents an approach to Air Navigation Services (ANS) cybersecurity and information system resilience involving a proposal for the air traffic safety electronics personnel (ATSEP) role in tactically and strategically addressing cyberattacks.

The aim is for air navigation services providers (ANSP) to attain and incorporate their technical capacity through the ATSEP expertise to address cybersecurity attacks to the Communication, Navigation, Surveillance/Air Traffic Management (CNS/ATM) systems.

International Federation of the Air Traffic Safety Electronics Associations (IFATSEA)'s recognition of the need for solid and forward-looking foundations for CNS/ATM systems/services resilience and continuity of service, is crucial. By proactively addressing cybersecurity challenges, rather than relying solely on reactive measures, ATSEPs can better safeguard critical ANS systems. This proactive approach ensures scalability and resilience as we navigate the ever-evolving landscape of cybersecurity threats to the aviation domain.

1. INTRODUCTION

1.1 As digitalization and networking continue to advance, the risk of cybercrime becomes more pronounced. International Civil Aviation Organization's (ICAO) Cybersecurity Action Plan and Aviation Cybersecurity Strategy provide valuable guidance, but there's room for improvement. Specifically, a need for air navigation services providers (ANSPs)' systems that will empower the ATSEP as the first responders to technical failures whether caused by equipment, software, hardware issues, or successful cybersecurity breaches. Early detection of a cybersecurity breach by the ATSEP is an approach that can positively influence the safety and economics of an ANSP through the tactical addressing of the cyberthreat either in the signal in space or ground CNS systems and services.

1.2 Advanced and legacy systems often lack inherent cybersecurity considerations, leading to a hybrid technological environment. The ATSEP plays a crucial role in ensuring the availability, integrity, accuracy, reliability, and continuity of aviation services in this diverse hybrid aviation environment. Annex 10 — *Aeronautical Telecommunications* of the Convention on International Civil Aviation (Chicago Convention) so far does not cover requirements for air traffic management (ATM) systems or address cybersecurity and IFATSEA believes that it should be updated. This update should include a requirement for technologies, systems, and tools that enable the ATSEP in differentiating between technical failures due to cyberattacks and typical failures, allowing for appropriate mitigation measures to be taken.

2. DISCUSSION

2.1 The world's aviation system is facing an increasing number of sophisticated cyber threats from various sources, including autonomous hackers and government-backed entities. The result of a cyberattack will be experienced by the ANSP as a technical failure impacting the nominal operation of CNS/ATM systems and services. Communication systems and protocols, particularly for legacy Air Navigation Systems, were not developed with security in mind. The interdependence among systems and the resulting combination of threat vectors poses a significant challenge for cybersecurity.

2.2 The role of the ATSEP during a cybersecurity event that leads or will lead to a CNS/ATM system or service malfunction should primarily focus on keeping the ATM/ANS system safe and resilient. By learning from each incident, refining protocols, and implementing best practices, the ATM/ANS community can better safeguard these critical infrastructures.

2.3 To timely and tactically address cyber-related events, 24/7 coverage of cyber-related tasks and duties must be guaranteed. This does not mean that all cyber-related tasks must be performed all the time, but the detection of cyber events is something that needs to be completed on a continuous and constant basis. In the case of an established 24/7 coverage by system, monitoring and control (SMC) ATSEP at the ANSP, it is beneficial to explore tasks that can be performed by these ATSEPs. To do this, an adequate level of expertise, combined with cybersecurity detection and decision-making support tools for the ATSEP work package, is needed to interpret classify, mitigate, and recover cyber-related events. It is common knowledge that the CNS/ATM systems must be minimally connected and even separated as possible from ANSP's administrative or economic networks as this reduces the vulnerability of safety and non-safety critical network environments. This is especially evident in the case of Cloud Service Providers, where, if implemented, there will be safety-critical interdependence on services across borders.

2.4 On the appearance of any degradation, the ATSEP on duty will have to identify whether it is due to a common technical failure or a cybersecurity attack. However, attack vectors can be either on the signal in space (Spoofing or Jamming) and/ or over the IP networks (e.g., DoS) or combined.

2.5 In the European Union Agency for Cybersecurity (ENISA)'s study on Securing Smart Airports there is a scenario provided by IFATSEA of drone intercept as a mobile vehicle for jamming and spoofing aircraft-airport and air traffic control-aircraft communications[1]. This scenario describes a spoofing attack that impacts ATM systems and automatic dependent surveillance — broadcast (ADS-B) communications. However, specific tools for the ATSEP working position to address such an attack, apart from manual ad-hoc improvisation by ATSEP and air traffic controllers (ATCOs) have not been identified or addressed yet.

2.6 To address such a combined attack, the ATSEP on duty must have the tools to identify whether a spoofing or jamming attack is taking place. Correspondingly the ATCO on duty needs to be

[1] https://www.enisa.europa.eu/publications/securing-smart-airports

familiar with the related procedures to identify the same issue. Moreover, once the detection phase of spoofing or jamming has been completed, the ATSEP must identify the source and the location of the attacker and coordinate with the competent authorities to resolve the issue. Currently, it is not possible to address the attack in an organized manner recorded in a response plan.

2.7 In the case of a combined attack both on the signal in space and over the networks, the ATSEP must be equipped/supported with appropriate decision-making and detection tools. Total system awareness is very difficult to maintain under such a combined cybersecurity attack. Speedy recovery to nominal operations would be a major enabler to the continuity of CNS/ATM Systems and services to airspace users. Although the recent event of Microsoft's update was not a cybersecurity event, it does show the vulnerability of the worlds aviation system. Whereas it also sheds the light of the need to be technically prepared for out-of-the-box solutions, something that only the humans can do.

2.8 Threats can be local or distributed, with the most dangerous being a distributed collection of events. Individually, these events may appear innocuous, but when considered as a whole, they could allow for a zero-day attack vector. Detecting such scenarios requires sharing data and utilizing pattern recognition algorithms at both local and global levels. These situations can be related to airspace, IT, infrastructure/installations, access control systems, or intrusion detection systems, either individually or in combination. The use of Artificial Intelligence (AI) supported tools to proactively identify and tactically address cyber security threats has been proposed in detail by IFATSEA in the 39th Session of the ICAO Assembly in 2016 (A39-WP/370: *A cybersecurity architectural approach for legacy- and SWIM-based CNS/ATM systems*)

2.9 While risk assessment and regulation of IT in ATM has been addressed, the practical means and tools to tactically address cyberattacks on CNS/ATM systems/services for all phases of the attack, especially the tactical/ recovery phase have not been sufficiently addressed. Although very good reference to the organizational part for ANSPs is elaborated at ICAO, not much information is found on the technological framework that the industry must work to address the unique and demanding aviation environment (ground, space and airspace). To enable the ATSEP to address cyberattacks proactively, special tools will need to be identified and considered during contingency planning.

2.10 The current approach for protecting the air navigation systems (ANS) and facilities focuses on detecting, responding and recovering from incidents. This approach leverages human factors as enablers supported by cyber-secure CNS/ATM systems that must be developed by design and open legacy CNS/ATM systems. Building a toolset for the intermediate layer of the ATSEP working position for the Systems Monitoring and Control of ATM/ANS systems and services can be a very efficient and cost-efficient approach.

2.11 Cybersecurity events that impact the technical aspect of CNS/ATM systems ultimately fall under the responsibility of the ATSEP. The ATSEP has been trained, certified and the only one authorized to make any changes at the CNS/ATM system operational level. They have also received training in the safety aspects of these systems and the implications on air traffic operations. The ATSEP is the first line of defence, ensuring the safety and resilience the ATM/ANS system.

2.12 CNS/ATM system manufacturers, including those with distributed architectures like Remote Towers, have already anticipated this need and developed system-specific cybersecurity tools for the ATSEP working position in the SMC domain. However, while these tools are valuable and welcome, they remain too system specific. A more harmonized and standardized approach, driven by ICAO, is necessary, ensuring that specific tools and training are available for the ATSEP working position. This would empower humans to address cybersecurity issues alongside other technical failures thus ensuring continuity and speedy recovery for better safety and reduced cost.

2.13 Access to equipment in the CNS/ATM system is restricted by national regulation to authorized ATSEPs only. Certain cybersecurity-related tasks can therefore only be performed by ATSEPs, as they are the only ones authorized and trained to comprehend the safety impact of any system change. ATSEPs understand the safety impact on the total system, so global system awareness at the ATSEP WP is necessary. For instance, patching systems to handle vulnerabilities is an ATSEP task because it requires access to operational equipment. These tasks can significantly increase the workload of ATSEPs, as they can be as urgent, serious, and impactful as any other system malfunctions.

2.14 Entry qualifications and competency schemes, including ATSEP Competency Based Training and Assessment, must be continually updated to cater for the specific needs of future tasks involving new technologies. Buy-in from other safety-critical or transport industries may also prove useful. Looking at the rail, road or the nuclear industry means to address cybersecurity events and contingencies and related technical failures may be beneficial.

2.15 Cyber incidents emphasize the need for robust training programs that address cybersecurity risks specific to ATC professionals. This training must include IT as well as ATSEP instructors and cover topics such as phishing awareness, secure password management, incident reporting procedures, and best cybersecurity practices. Regular refresher courses and updates on emerging threats are essential to maintain high levels of situational awareness and cybersecurity resilience. Effective ATSEP training and continuous education play a critical role in enhancing cybersecurity awareness and preparedness.

2.16 Reporting of cybersecurity incidents must be prompt, and ATSEP professionals need to be encouraged to engage in this activity. Establishing a culture of reporting, without fear of blame or disciplinary actions, can help identify and respond to threats effectively. Timely reporting and information-sharing contribute to early detection and mitigation of cyber incidents, minimizing potential harm to the overall system. Encouraging a proactive reporting culture is essential for maintaining cybersecurity resilience.

2.17 A cost-effective approach considers the particularities of the CNS/ATM environment and the safety and time criticality of ATM/ANS services. It is not addressed purely as an IT Security project but rather with a holistic approach that encompasses airspace-related, IT-related and infrastructure/installations aspects, including access control systems tailored to the ANS environment. Certain cybersecurity-related tasks can only be performed by ATSEPs, as they are the only ones authorized and knowledgeable about the safety impact on the total system.

3. CONCLUSION

3.1 In the forthcoming automation era, ANSPs will face significant challenges in addressing issues such as cascade failures due to a cyberattack which are a potential reality due to the tight coupling, interoperability and interrelation of the new systems and processes. Training the current ATSEP workforce to cybersecurity elements when addressing CNS/ATM systems (space and ground) will be highly cost-effective, with the only cost being the additional training for ATSEPs. Acquiring basic competencies in handling cyber issues within the safety-critical environment of CNS/ATM systems and services will expedite the tactical and strategic functions and cooperation with cyber-experts (when needed) for both online and offline systems, whether they are attacked or infected. systems. Expensive IT cyber experts will only be necessary when (and if) needed.

3.2 ICAO’s consideration of the proposals presented by IFATSEA for ATSEP working position functionalities, aimed at addressing cyber threats, could be a significant step toward guiding the industry in providing harmonized and interoperable products for ANSPs. This would enhance the intrinsic capabilities of evolving ANS/ATM systems at minimal cost.

3.3 The work performed by ATSEPs is critical to the safety and efficiency of the world's air navigation systems/services. Air traffic controllers and pilots rely on the Communication, Navigation, Surveillance/Air Traffic Management (CNS/ATM) systems that ATSEPs install and maintain. Given the high-impact and high-consequence nature of their work, ATSEPs play a vital role in ensuring safety. Cybersecurity training for ATSEPs is essential to the sustainability of the world's air navigation system. The tasks ATSEP perform are life critical.

— END —