Strengthening Aviation Cybersecurity with Security Operations Centres

Wesley Murisa and Marijke Coetzee
North-West University, Potchefstroom, South Africa

wesmur@gmail.com
marijke.coetzee@nwu.ac.za

Abstract: Even though cybersecurity is a top priority for the aviation industry, research indicates that there are still many challenges to address. Modern aviation systems encompass cloud computing, OT, IoT, mobile devices, and traditional IT infrastructure. The network complexity has expanded the attack surface, leading to an increase in security incidents. Due to this complexity, detecting security incidents on time is challenging. Research indicates that it may take up to 196 days to detect an incident and another 56 days to address it, highlighting the urgency of improving security response. In this regard, establishing Security Operations Centres (SOCs) in the aviation sector must be addressed. SOCs can be instrumental in reducing the time it takes to detect and respond to security incidents. They provide visibility into threats, aid investigations, and enhance forensic efforts, enabling proactive threat mitigation. Research has been carried out on SOC implementations for specific domains like IoT, mobile devices, and higher education, neglecting aviation systems. Aviation systems such as Air Traffic Management (ATM) face unique security vulnerabilities, including signal modification, jamming, flooding, data and command injection, GPS spoofing, and blocking attacks, primarily due to their reliance on wireless technology. Most of these wireless technologies do not use encryption or authentication because they were designed to maximize performance. Insufficient funding also negatively affects ATM systems, resulting in the wide use of legacy ATM systems and a shortage of skilled personnel. ATM systems are considered critical infrastructure frequently targeted by well-resourced threat actors, including terrorists and nation-state actors, necessitating higher protection levels. This paper motivates the development of a customised SOC implementation framework for ATM systems to enhance aviation security by increasing visibility into threats and facilitating timely remediation.

Keywords: Critical infrastructure, Aviation, Air traffic management (ATM), Security operations centre (SOC)

1. Introduction

Air Traffic Management (ATM) systems have been known to be vulnerable to network security threats like signal modification and jamming, data and command injection, GPS spoofing, and blocking attacks mainly because they rely on open wireless technology (Dave *et al.*, 2022). Previously, these vulnerabilities did not pose significant safety and security challenges because ATM systems were custom-made and standalone. Today, ATM systems are massively integrated with non-aviation systems, increasing the risks of life-threatening cyber-attacks. Security vulnerabilities in ATM systems are high because civilian aviation systems do not use encryption by default to reduce operational overheads. ATM system vulnerabilities are also amplified by the failure to upgrade legacy systems in a timely manner due to the exorbitant costs of upgrading and the shortage of skilled personnel (Kagalwalla & Churi, 2019). Further, ATM systems are viewed as critical infrastructure and are often targeted by threat actors, including terrorists and well-resourced nation-state actors; hence, they require higher protection.

Security Operations Centers (SOC) have been widely recognised as an effective tool for improving cyber security in organisations, especially nowadays when the rate of cyber security threats continues to escalate across private and public sectors worldwide (Kokulu *et al.*, 2019). SOCs mainly provide visibility of security threats across the organisation, enabling forensic investigations and timely remedial action. Visibility is achieved by collecting security logs from technical controls and critical assets into a central database, which are continuously analysed to identify security incidents. Analysts are alerted when security incidents are identified. The analysts, often members of the Cyber Incident Response Team (CIRT), investigate the alerts further and take corrective action where necessary (Majid & Ariffi, 2019). SOCs can go a long way in addressing ATM cyber security challenges.

This paper is structured as follows: Section 2 discusses Air Traffic Management systems. This is followed by an outline of cyber security challenges in ATM systems in section 3. Section 4 describes SOCs before considering the current state of the art of SOCs in section 5. Section 6 discusses the recommendations for implementing SOCs for ATMs. Lastly, a concussion is given in section 7.

2. Air Traffic Management Systems

Aviation is a complex critical infrastructure system comprising different sub-systems, including ATMs, airports, and airlines (Lykou, Iakovakis & Gritzalis, 2019). ATM systems are at the core of air traffic management services. Three subsystems, namely, Communication, Navigation and Surveillance (CNS), comprise ATM systems(Lu *et al.*, 2021). Communication systems are responsible for voice and message communication between Air Traffic Control (ATC) and aircraft. In addition, pilots use communication systems to exchange information. Navigation systems are used to determine location during transit and landing. Lastly, the purpose of surveillance systems is to track an aircraft's location. The three ATM sub-systems described above, combined with Aeronautical Information Services (AIS) and meteorological services, provide information ATC uses to manage and guide aircraft (Stelkens-Kobsch, Finke & Carstengerdes, 2017). The diagram below shows how these systems are combined to give ATC a unified display system for directing and controlling aircraft.

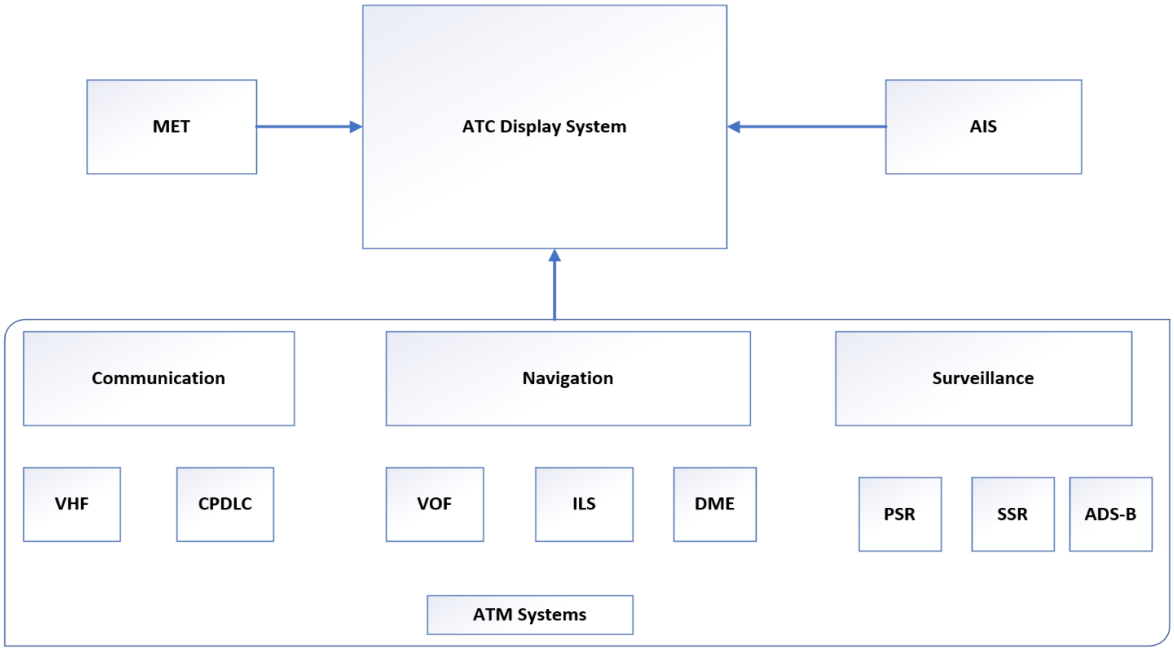

Figure 1: Air Traffic Management systems

ATM communication is based on two wireless technologies: Very High Frequency (VHF) and Controller Pilot Data Link Communication (CPDLC) systems. VHF is the primary means of communication between ATC and pilots and uses voice. It also broadcasts additional information like weather updates (Dave *et al.*, 2022). Limited range and lack of authentication are the major shortcomings of VHF. The absence of authentication on VHF makes it susceptible to denial of service and eavesdropping attacks. CPDLC is a message-based alternative to VHF that is considered more efficient, faster, and easier to use (Gurtov, Polishchuk & Wernberg, 2018). It helps reduce congestion on VHF when there are high traffic volumes and offers backup when VHF is out of range. Like VHF, it does not use authentication, making it vulnerable to several wireless attacks.

Navigation systems comprise VHF Omnidirectional range (VOR), Instrument Landing System (ILS), and Distance Measuring Equipment (DME), which are used to guide an aircraft in transit and during landing (Dave *et al.*, 2022). As the name indicates, VOR uses VHF to determine an aircraft's location relative to beacons on the ground during transit. ILS is a non-precision approach system that guides planes to the runway when conditions are unsuitable for visual landing (Sathaye *et al.*, 2019). Like VOR, ILS is fixed on the ground and uses radio signals and high-intensity light arrays to guide the pilot to the runway. DME is used with VOR to provide the pilot with navigation information during a flight.

Primary Surveillance Radar (PSR), Secondary Surveillance Radar (SSR), and Automatic Dependent Surveillance-Broadcast (ADS-B) make up surveillance systems. PSR is a passive and independent surveillance system that uses a rotating radar to detect the direction and distance of objects in airspace (Habler, Bitton & Shabtai, 2022). SSR is another surveillance system that differs from PSR in that it depends on the target aircraft to respond to its interrogative messages, for it determines an aircraft's altitude, speed, and destination (Lykou, Iakovakis & Gritzalis, 2019). PSR and SSR are similar in using radio signals to locate target aircraft details. ADS-B is the third method that is used for surveillance purposes in ATMs. In ADS-B, aircrafts continuously broadcast

their identity, location, and speed to ground stations and other aircrafts (Haass, Craiger & Kessler, 2018) . The aircraft uses the Global Navigation Satellite System (GNSS) to determine its location and velocity before sending that information to ground stations and other aircraft.

Data from the CNS systems described above is transmitted to networked computer systems, often running proprietary operating systems for storage, processing, and further transmission to the ATC display system (Lu *et al.*, 2021). Traditionally, these networks used the concept of segregation and operating system hardening to provide security against unauthorised access. Whilst segregation can be effective for providing protection, configuration errors can expose ATM networks to security threats in the local area network connected to the internet. The requirement to connect ATM systems to third parties, such as providers of meteorological data and AIS, exposes the supposedly closed network to further security risks.

The life span of ATM systems can be as long as 20 years (de Haan & Youssouf, 2023). The primary reason for the long life span is that ATM systems are critical infrastructures that are heavily regulated. New systems are subjected to rigorous validation efforts to ensure safety and reliability. In addition, the development cycles of ATM systems are lengthy and costly. Further, there is a reluctance to change critical infrastructure like ATM systems because they constantly operate, and there is little appetite for downtime. As a result, most ATM systems run on legacy systems with many vulnerabilities that malicious actors can easily exploit. Security challenges caused by legacy systems and other aspects of ATM systems are analysed in detail in the next section.

3. Air Traffic Management Security Challenges

After describing ATM systems in Section 2, this section discusses their cyber security challenges. The aviation industry is a lucrative target for cybersecurity criminal groups motivated by financial gain, as evidenced by the general increase in cybersecurity attacks over the past few years. On the one hand, terrorist groups find aviation a suitable target because successful attacks are fatal. On the other hand, national state actors also target aviation systems for intellectual property theft, intelligence gathering and political reasons. Disgruntled employees complete the list of high-profile threat actors targeting aviation systems. Therefore, ATM systems are always at risk of attack from threat actors mentioned above. The most prominent cyber security challenges in ATMs are detailed below.

Insecure by design

Most of the cyber security challenges in ATMs emanate from the lack of security considerations in the initial system design, mainly because cyber security threats were not prevalent when they were developed (Dave *et al.*, 2022). However, information security best practices require that requirements be included in the system lifecycle's design, implementation, and maintenance phase. Attempting to address security limitations after systems development is often very expensive and may introduce new security problems and system errors. The best way to address this challenge is by developing a new system that incorporates security requirements from the onset.

Unencrypted, wireless communications

Most ATM technologies use clear-text wireless communication, which cannot provide confidentiality, integrity, and non-repudiation. Although some ATM systems used by the military now use encryption, their civilian counterparts are still not encrypted due to the need to reduce operational overheads. Many ATM systems are known to be vulnerable to network security threats like eavesdropping, signal modification and jamming, data and command injection, GPS spoofing and blocking attacks mainly because they rely on unencrypted wireless technology. The availability of cheap tools such as Software Defined Radio (SDR) (Lu *et al.*, 2023) has made attacking these unencrypted wireless ATM systems easier.

Enlarged attack surface

Inherent security risks in ATM systems described above are amplified by the need to integrate aviation systems with non-aviation systems, core networks and cloud systems connected to the internet (Lu *et al.*, 2021). Air Navigation Service Providers (ANSPs), airlines, airports, and aircraft systems now share data to improve service to their tech-savvy aviation customers (Ukwandu *et al.*, 2022). The integration enlarges networks and creates new attack vectors in systems that previously relied on closed networks and proprietary protocols for security (Bernsmed *et al.*, 2022). A radical move from the view that ATM systems are closed and secure must be adopted when assessing cyber security risks.

Complex architecture

Increased interconnection and integration of aviation systems described above create a complex architecture which is difficult to secure. The result of integrations is adding external networks and their vulnerabilities to an already complex aviation sector network. Most players in the aviation sector use different technologies, including Operations Technology (OT), Internet of Things (IoT) and cloud applications supported by various supply chain partners (Kagalwalla & Churi, 2019). Other nations like the US use rail at airports, introducing an additional node to an already complex ecosystem (Szyliowicz, 2004). Although it can be argued that integrating systems improves air traffic control systems, the security risks brought about by these complexities must not be overlooked.

Legacy systems

Legacy systems, in the form of outdated technology and software, do not receive security patches once they have reached their end of life. Original Equipment Manufacturers (OEMs) and system developers often stop supporting systems that have been discontinued and as a result, use insecure protocols. This creates vulnerabilities that threat actors can easily exploit. The risks will be minimal if these legacy systems are isolated or in closed networks but as mentioned before, ATM networks are integrated with external networks. Moreover, most ANSPs are owned by national governments, which do not provide adequate funding for frequent system upgrades. As a result, most ATMS systems in use are legacy systems vulnerable to cyber security attacks.

Shortage of skilled cyber security personnel

The availability of skilled cyber security personnel in ATMs directly relates to the sector's financial situation. High demand for cyber security specialists worldwide results in the most funded sector getting the most available skills. Due to the financial challenges in the aviation sector, it isn't easy to attract and retain qualified and experienced security personnel, thereby affecting the implementation of cybersecurity programs. As a result, cyber security implementation in the aviation sector has not yet matured, although there is awareness of the importance of cyber security. This leaves the aviation sector inadequately protected and vulnerable to cyber security attacks. Statistics show that cyber security attacks in the aviation industry have increased significantly over the past few years.

Supply chain attack vectors

Other cyber risks in ATMs emanate from the supply side (Kandera *et al.*, 2022). Threat actors have devised ways of varying their attack methods by compromising aviation equipment and service suppliers. Attack vectors commonly used in aviation supply chains are software development tools, hardware components, and network connectivity. Threat actors utilise these vectors to inject malicious code into products under development or maintain remote network access. Once access has been obtained, the attackers retain it and use it to access targets in different countries serviced by that supplier. Vendors are often trusted and given remote access to their client's networks for support and maintenance. Therefore, a single attack on one supply chain partner can guarantee a threat actor access to many targets across different continents.

The challenges highlighted above expose ATMs to numerous cybersecurity threats, necessitating a comprehensive approach for mitigation. Strategies to tackle these cybersecurity challenges encompass developing secure ATM systems and the implementation of effective incident response protocols. The following section delves into the Security Operations Centre (SOC), a vital information security management tool that can enhance the overall security posture of ATMs.

4. The Security Operations Centre

SOCs are centralised security hubs established to bolster an organisation's security posture, swiftly identifying and responding to threats and security breaches before they disrupt core business operations (Majid & Ariffi, 2019). They are pivotal instruments offering comprehensive insight into security threats and attacks targeting an organization. The evolving complexity of operational landscapes, integrating diverse technologies within organizations, has made monitoring all security threats increasingly arduous (Mughal, 2022). Consequently, organizations encounter delays in recognizing and mitigating security incidents. For instance, research by Vielberth *et al.* (2020) reveals that it takes 196 days to detect an incident and an additional 56 days to address it. An effectively implemented SOC alleviates this issue by amassing logs from security controls and critical systems within the organisation, swiftly identifying threats in real-time.

SOCs are structured according to the People, Processes, and Technology (PPT) framework (Vielberth *et al.*, 2020) with Governance constituting another critical element that can be incorporated into the PPT framework.

People encompass personnel from various domains, including business, information technology (IT), and security analysts engaged in establishing and managing the SOC. Technology pertains to the technical tools deployed for data collection, analysis, and issuing security alerts upon detecting attacks. Governance and processes, on the other hand, encompass incident response playbooks, policies, procedures, and incident management protocols.

Security logs from technical controls and critical assets are funnelled into a Security Information and Event Management (SIEM) system to achieve visibility. The logs from all onboarded systems undergo ingestion, normalization, correlation, and analysis to pinpoint suspicious security events. Analysts receive notifications when such events are detected via the service desk system, and subsequent investigations determine whether the suspected events are true or false positives (Saraiva & Mateus-Coelho, 2022). False positives are closed within the service desk system, while true positives are subject to further investigation and remediation. Policies and procedures define the types of security incidents that analysts can handle independently and those that require a CIRT.

Maintaining visibility over threats and attacks targeting organisations is paramount, especially considering the vast array of technologies employed, ranging from cloud and on-premises systems to mobile and IoT devices (Miloslavskaya, 2016). The diversity of technologies, including ATMs, introduces complexities in monitoring and managing them effectively without the aid of a SOC. A SOC bolsters an organisation's security stance by enabling the centralized tracking of diverse technologies, even if they are geographically dispersed.

While the primary function of a SOC is to provide visibility into security threats, it also performs other essential functions. SOCs are crucial components of Cyber Security Incident Response Teams (CSRITs), aiding in threat detection, aggregating threat information across the network, and supporting forensic investigations. Another function of a SOC is to monitor security controls deployed within an organisation(Jacobs, Arnab & Irwin, 2013). This monitoring function enables organisations with a SOC to gain a centralized view of all security threats detected by security controls such as firewalls, Intrusion Prevention Systems (IPS), and antimalware systems. The SOC promptly detects the unavailability of any onboarded technical controls. Organizations are often legally mandated to retain logs for specific periods, a function efficiently fulfilled by a SOC. The UK government's Her Majesty's Government (HMG) mandates the establishment of a SOC (Onwubiko & Ouazzane, 2019). SOCs can also assist in meeting various compliance requirements, including laws and regulatory frameworks like GDPR, the POPI Act, PCI DSS, and ISO 27001.

SOCs are categorized as internal when operated by an organization's employees and external when managed by external service providers (Onwubiko, 2015). Many organizations opt for a hybrid model, where external service providers handle monitoring and alerting while the host organisation's IT engineers manage remediation functions. Challenges in attracting and retaining qualified cybersecurity experts may influence the choice between internal and external SOC models in attracting. Internal and external SOCs can be hosted on-premises or in the cloud.

Concerning architecture, organizations venturing into SOC establishment can choose between centralized, decentralized, and distributed architectures (Vielberth *et al.*, 2020). In a centralized SOC, logs from different locations or subsidiaries are sent to a central hub for processing. In the distributed architecture, SOCs are deployed in various locations or subsidiaries but appear as one integrated SOC to end users. Decentralized SOCs encompass a combination of distributed and centralized elements. They deploy SOCs with limited functionalities in diverse locations or subsidiaries, forwarding their data to a central SOC for processing. Specific business requirements should guide the choice of SOC architecture.

While much research has been conducted on SOCs, a limited focus has been on ATM systems. Existing research has explored SOC implementations for IoT and mobile devices (Suomalainen et al., 2022), SOC implementations in higher education (Gamilla & Palaoag, 2022), and visualization techniques to enhance SOC performance (Mihindu & Khosrow-shahi, 2020). Other research has aimed to improve SOC effectiveness by addressing critical asset onboarding and identifying challenges (Onwubiko, 2021). Notable systematic literature reviews (Schlette, Vielberth & Pernul, 2021) have generated recommendations for enhancing SOC effectiveness. Additionally, research has extensively explored ways to improve SOC analyst performance (Agyepong *et al.*, 2020). Jacobs, Arnab and Irwin (2013) has proposed a framework for measuring SOC services' effectiveness while Villalón-Huerta, Gisbert and Ripoll-Ripoll (2022) introducing a technology-independent defensive kill chain for incident response to detect and respond to threats.

5. Current State of the art on Aviation SOCs

After examining the role of Security Operations Centers (SOCs) in enhancing visibility into cybersecurity threats in ATMs, this section explores exemplary ATM SOCs worldwide that can serve as models for the African continent. SOCs support cybersecurity incident response and information-sharing initiatives in Europe and the United States. However, the implementation of SOCs in ATMs is not formally documented in academic research. Detailed insights into SOC utilization are provided below.

EUROCONTROL established the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) to proactively detect, prevent, respond to, and recover from cybersecurity attacks targeting ATM systems in Europe (Mana & Friligkos, 2019). EATM-CERT operates SOCs at local, national, and regional levels to bolster incident response teams (Lekota & Coetzee, 2021). EATM-CERT collaborates with national European CERTs to share relevant cybersecurity information related to ATMs. Additionally, EATM-CERT lends its expertise to various national CERTs to manage ATM-related cybersecurity incidents effectively. EATM-CERT employs a Malware Information Sharing platform to disseminate ATM cybersecurity threat intelligence across multiple European countries. Furthermore, EATM-CERT helps its members by offering guidelines for procuring SOC services and addressing the cybersecurity skills gap in ATM services.

In response to escalating cybersecurity threats against aviation systems in the US, the Aviation Information Sharing Center (A-ISAC) was established (A-ISAC, 2023). A-ISAC's membership includes airlines, airports, Original Equipment Manufacturers (OEMs), government CERTs, and ANSPs, all actively engaged in threat detection, prevention, and remediation. This collaboration involves sharing vulnerabilities, threat intelligence, policies, and standards on a secure, common platform. Each stakeholder operates its own SOC, gathering threat information shared among peers. Additionally, A-ISAC monitors the dark web and social media for additional threat intelligence. A-ISAC fosters information exchange through forums, including working groups and summits, where aviation cybersecurity experts convene to discuss critical topics.

The EATM-CERT and A-ISAC exemplify cutting-edge SOC implementations in addressing cybersecurity challenges in ATMs. EATM-CERT focuses on ATM-specific solutions, while A-ISAC caters to the broader aviation industry. Nevertheless, both approaches provide valuable insights for establishing effective SOCs in African ATM systems. The subsequent section outlines recommendations for implementing SOCs in African ATMs.

6. Security Operations Centre for Air Traffic Management

Addressing cybersecurity vulnerabilities in critical infrastructures such as ATMs is crucial to ensuring safety and safeguarding human lives. The urgent attention needed to tackle the lack of security in most ATM systems cannot be overstated, as successful attacks on these systems can have fatal consequences. While efforts are underway to develop more secure ATM systems, the lengthy development cycles and rigorous testing protocols necessary before implementation mean that existing security flaws will persist for some time. This underscores the pressing need to confront cybersecurity challenges in ATMs. SOC capabilities can address ATM challenges directly and indirectly as summarised in the table 1 below.

Sophisticated and resourced threat actors already target ATM systems because they are critical infrastructure. Security challenges such as legacy systems, insecure by design, complex architecture, enlarged attack surface and supply chain attack vectors, make ATM systems more vulnerable to cyber security threats. These challenges are directly addressed by a SOC through automated threat monitoring. Automated threat monitoring provides visibility of the attacks and supports incident response teams. Auto remediation rules set in SOCs resolve security incidents as soon as they are identified without manual intervention. Furthermore, storing security logs aligns with the compliance requirements of different security governance frameworks such as NIST and support forensic investigations.

In SOCs, all critical systems and security control send logs to the SIEM to detect security threats, as described in Section 4. Onboarding these systems provides a clear picture of the systems in use and structure of ATM networks, thereby indirectly addressing the complex architecture challenge described in section 3. Documenting systems in use and their relationships can be easily achieved when planning the systems to be onboarded to a SOC because all systems are identified and documented. Network documentation can be helpful for evaluating and simplifying the network structure. In addition, security alerts from the SOC will provide insight into which part of the network is most vulnerable and requires urgent attention.

Implementing SOCs in ATMs also forces the sector to indirectly address skilled cyber security manpower challenges. SOCs require skilled cyber security personnel. Therefore, management is forced to find a solution to this problem. The problem can be addressed in different ways, including outsourcing, training, headhunting and attracting skilled personnel through lucrative remuneration. Despite the method chosen to address the

skill shortage, the sector benefits from the availability of skilled and experienced personnel. SOC functions such as automated remediation of security threats can be handy in addressing human resources challenges. This will result in the maturity of cybersecurity management programs and reduce security threats in the long run.

While implementing a SOC in ATM systems can go a long way in addressing cybersecurity challenges in the sector, the costs involved are huge and underfunded ANSPs may struggle to finance setting up a full-fledged SOC all at once (Vaarandi & Mases, 2022). SOC building blocks, such as building the cyber security skill base and implementing an SIEM, can be achieved relatively cheaply before an entire SOC can be set up. While these two steps will not provide as much benefit as setting up a SOC, they are critical components of a SOC that provide some protection while preparing for full SOC implementation.

An additional impediment to effectively addressing ATM cyber security challenges through SOCs lies in the limited knowledge and awareness of cyber security challenges by aviation stakeholders. A survey by (Strohmeier *et al.*, 2019) reveal a gap in appreciation of the potential impact of cyber security on Air Traffic Control (ATC) technology although some progress has been noted in Europe. The authors characterise aviation stakeholders response to cybersecurity issues as defensive and secrecy. Consequently, it is imperative to bridge the cybersecurity knowledge gap among stakeholders to ensure the viability of SOCs as a solution to ATM cyber security challenges.

Table1: Mapping of ATM cyber security problems to solutions provided by SOCs

ATM security challenges	SOC Solutions
Insecure by design	Automated threat monitoring Auto-remediation Support for incident response activities and forensic
Unencrypted, wireless communications	
Enlarged attack surface	
Legacy systems	
Supply chain attack vectors	
Shortage of skilled cyber security personnel	Auto-remediation and Outsourcing
Complex architecture	Network Documentation

Although research on SOCs has been conducted in various contexts, such as mobile devices and higher education, ATM systems pose unique challenges as critical infrastructures that blend Operations Technology (OT) systems like PSR with computer networks to provide services to ATC. The ATM network frequently integrates with external systems such as meteorological information service providers and AIS. Additionally, systems like CPDL expand ATM networks to aircraft and airline networks. The attack surface is further broadened by providing remote support and maintenance access to supply chain partners. Further, cloud systems and mobile devices are integrated into the same networks. This calls for a unique approach to obtaining the best out of using SOCs to curb cybersecurity threats in ATMs.

7. Conclusion

ATM systems are vulnerable to cyber security threats from different actors motivated by different reasons. Security challenges described in section 3 make it easier for threat actors to exploit ATM systems vulnerabilities, but SOCs can provide threat visibility and support incident response activities. While lessons can be learned from the current state of the art described in section 5, the African continent does not have fully functional cyber security structures on a continental level, as in the US and Europe. A formalised approach that guides the implementation of SOCs for ATM systems is required, as has been done for other sectors like higher education. Such an approach should consider the ATM system-specific challenges like legacy systems, complex architectures, shortage of skilled manpower, inadequate funding and enlarged attack surface. Africa can learn from the US and Europe by pulling resources and establishing SOCs at a continental level. Skilled cyber security experts can be employed at a continental level and support all member states. Such an initiative can go a long way in reducing the prevalence of security incidents on ATM systems on the continent.

References

A-ISAC. 2023. *A-ISAC* https://www.a-isac.com/ Date of access: 05 November 2023.

Agyepong, E., Cherdantseva, Y., Reinecke, P. & Burnap, P. 2020. Towards a framework for measuring the performance of a security operations center analyst. In. 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland. pp. 1-8.

Bernsmed, K., Bour, G., Lundgren, M. & Bergström, E. 2022. An evaluation of practitioners' perceptions of a security risk assessment methodology in air traffic management projects. *Journal of Air Transport Management*, 102:102223. 10.1016/j.jairtraman.2022.102223

Dave, G., Choudhary, G., Sihag, V., You, I. & Choo, K.-K.R. 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, 112:102516. 10.1016/j.cose.2021.102516

de Haan, J. & Youssouf, A. 2023. Cryptography Based Security for the ATM Surveillance Chain. In. 2023 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), Melbourne, Australia. IEEE. pp. 31-36.

Gamilla, A.P. & Palaoag, T.D. 2022. Building a Barrier: A security operations center framework for a sustainable smart campus network. In. 2022 6th International Conference on Information Technology (InCIT), Nonthaburi, Thailand. pp. 256-261.

Gurtov, A., Polishchuk, T. & Wernberg, M. 2018. Controller–Pilot Data Link Communication Security. *Sensors*, 18(5):1636. 10.3390/s18051636

Haass, J.C., Craiger, J.P. & Kessler, G.C. 2018. A Framework for Aviation Cybersecurity. In. NAECON 2018 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA. pp. 132-136.

Habler, E., Bitton, R. & Shabtai, A. 2022. Evaluating the Security of Aircraft Systems. *arXiv preprint arXiv:2209.04028*, 10.48550/arXiv.2209.04028

Jacobs, P., Arnab, A. & Irwin, B. 2013. Classification of security operation centers. In: HS Venter, M.L.a.M.C., ed. 2013 Information Security for South Africa, Sandton, South Africa. pp. 1-7.

Kagalwalla, N. & Churi, P.P. 2019. Cybersecurity in aviation: An intrinsic review. In. 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India. pp. 1-6.

Kandera, B., Holoda, Š., Jančík, M. & Melníková, L. 2022. Supply chain risks assessment of selected EUROCONTROL's surveillance products. In. 2022 New Trends in Aviation Development (NTAD), Novy Smokovec, Slovakia. pp. 86-89.

Kokulu, F.B., Shoshitaishvili, Y., Soneji, A., Zhao, Z., Ahn, G.J., Bao, T. & Doupé, A. 2019. Matched and mismatched SOCs: A qualitative study on security operations center issues. In. Proceedings of the ACM Conference on Computer and Communications Security, London United, Kingdom. pp. 1955-1970.

Lekota, F. & Coetzee, M. 2021. Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice. In. European Conference on Cyber Warfare and Security, Online. Academic Conferences International Limited. pp. 507-XII.

Lu, X., Dong, R., Wang, Q. & Zhang, L. 2023. Information Security Architecture Design for Cyber-Physical Integration System of Air Traffic Management. *Electronics (Switzerland)*, 12(7), 1665. 10.3390/electronics12071665

Lu, X., Wu, Z., Wu, Y., Wang, Q. & Yin, Y. 2021. Atmchain: Blockchain-based solution to security problems in air traffic management. In. 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA. pp. 1-8.

Lykou, G., Iakovakis, G. & Gritzalis, D. 2019. Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies*:245-260. 10.1007/978-3-030-00024-0_13

Majid, M. & Ariffi, K. 2019. Success factors for cyber security operation center (SOC) establishment. In. Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, 18 July 2019, Bandung, Indonesia, Bandung, Indonesia.

Mana, P. & Friligkos, V. 2019. Eurocontrol/Eatm-Cert Services - Supporting Aviation To Better Manage Cyber Threats. In. 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA. pp. 1-15.

Mihindu, S. & Khosrow-shahi, F. 2020. Collaborative visualisation embedded cost-efficient, virtualised cyber Security operations centre. In. 2020 24th International Conference Information Visualisation (IV), Melbourne, Australia. pp. 153-159.

Miloslavskaya, N. 2016. Security operations centers for information security incident management. In. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria. pp. 131-136.

Mughal, A.A. 2022. Building and Securing the Modern Security Operations Center (SOC). *International Journal of Business Intelligence and Big Data Analytics*, 5(1):1-15.

Onwubiko, C. 2015. Cyber security operations centre: security monitoring for protecting business and supporting cyber defense strategy. In. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (cybersa), London, UK. pp. 1-10.

Onwubiko, C. 2021. Rethinking security operations centre onboarding. In. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland. pp. 1-9.

Onwubiko, C. & Ouazzane, K. 2019. Challenges towards building an effective cyber security operations centre. *International Journal on Computational Science & Applications*, 4(1):11-39. 10.48550/arXiv.2202.03691

Saraiva, M. & Mateus-Coelho, N. 2022. CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Computer Science*, 204:961-972. 10.1016/j.procs.2022.08.117

Sathaye, H., Schepers, D., Ranganathan, A. & Noubir, G. 2019. Wireless attacks on aircraft landing systems. In. Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami Florida. pp. 295-297.

Schlette, D., Vielberth, M. & Pernul, G. 2021. CTI-SOC2M2–The quest for mature, intelligence-driven security operations and incident response capabilities. *Computers & Security*, 111:102482. 10.1016/j.cose.2021.102482

Stelkens-Kobsch, T.H., Finke, M. & Carstengerdes, N. 2017. A comprehensive approach for validation of air traffic management security prototypes: A case study. In. 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), St. Petersburg, FL, USA. pp. 1-10.

Strohmeier, M., Niedbala, A.K., Schäfer, M., Lenders, V. & Martinovic, I. 2019. Surveying aviation professionals on the security of the air traffic control system. In. Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers, Barcelona, Spain. pp. 135-152.

Szyliowicz, J.S. 2004. Aviation security: promise or reality? *Studies in conflict & terrorism*, 27(1):47-63. 10.1080/10576100490262160

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... Bellekens, X. 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, 13(3):146. 10.3390/info13030146

Vaarandi, R. & Mases, S. 2022. How to build a SOC on a budget. In. Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022, Rhodes, Greece. pp. 171-177.

Vielberth, M., Bohm, F., Fichtinger, I. & Pernul, G. 2020. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 8, 10.1109/ACCESS.2020.3045514

Villalón-Huerta, A., Gisbert, H.M. & Ripoll-Ripoll, I. 2022. SOC Critical Path: A Defensive Kill Chain Model. *IEEE Access Volume 10*, 10:13570-13581. 10.1109/ACCESS.2022.3145029