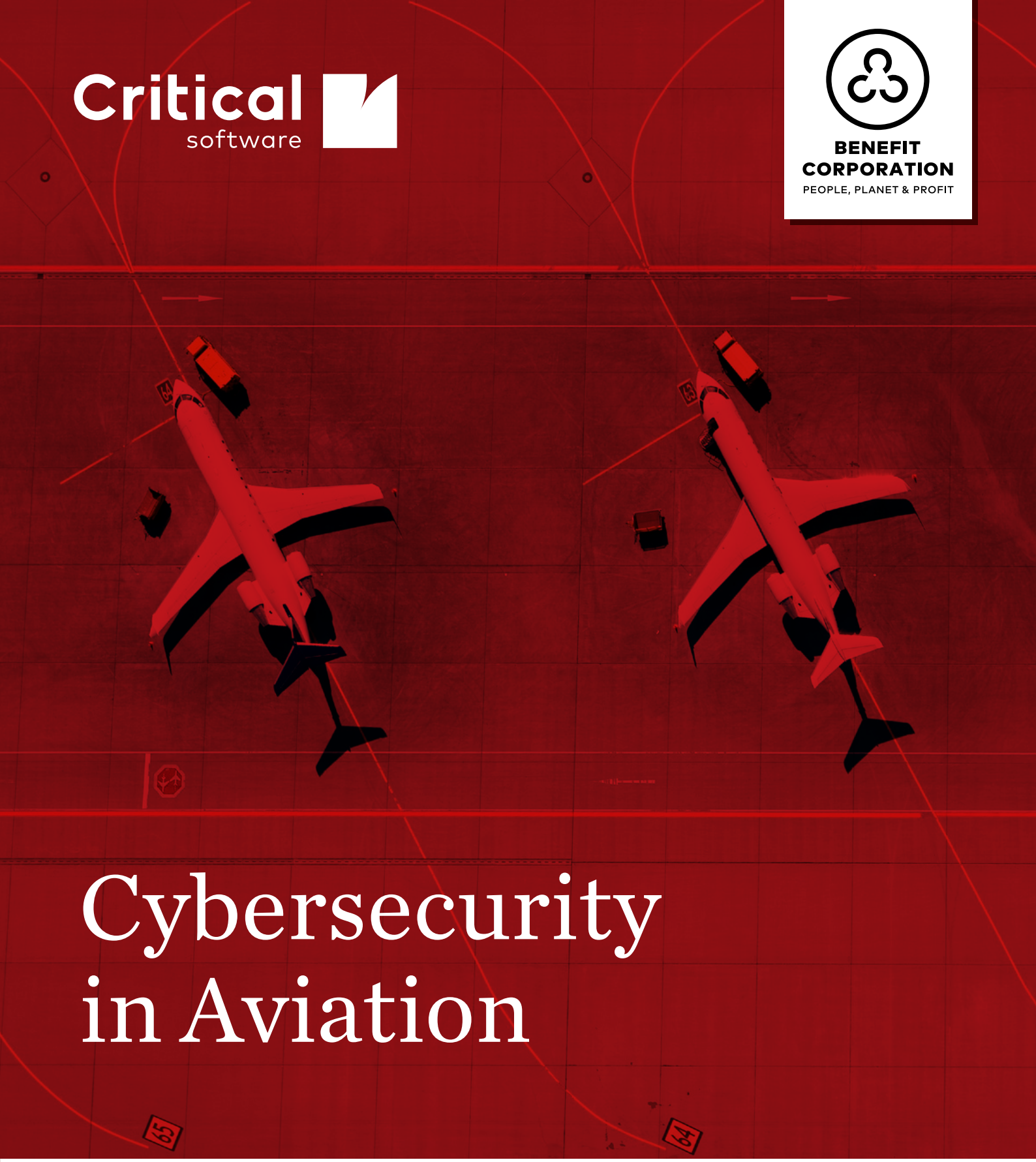
Critical software

BENEFIT CORPORATION
PEOPLE, PLANET & PROFIT



Cybersecurity in Aviation

Addressing Cybersecurity Challenges in Modern Aviation Systems

criticalsoftware.com
info@criticalsoftware.com

What is Cybersecurity

Cybersecurity encompasses a comprehensive set of practices, strategies, and technologies designed to safeguard systems, networks, and data from digital threats and unauthorized access. In an era marked by rapid digital interconnectivity, cybersecurity has become a fundamental pillar in safeguarding the confidentiality, integrity, and availability of information (Werthwein, Brunner, & Annighoefer, 2023). It plays a crucial role in not only protecting sensitive data and maintaining privacy but also ensuring the uninterrupted functioning of operations across various sectors.

Cybersecurity relies on several key methods to protect systems and data (Wadho, 2023):

1. Encryption plays a fundamental role by converting data into a secure format, keeping it unreadable to unauthorized users.

2. Firewalls act as protective barriers, filtering network traffic to prevent harmful or unauthorized access.

3. Strong authorization protocols add an extra layer of security, requiring multiple verification steps before access is granted.

4. Intrusion detection systems enhance network protection by monitoring network activity and identifying potential threats, helping ensure that only trusted and authorized devices maintain access.

5. Periodic security assessments and staff training are essential for identifying vulnerabilities and ensuring an effective response to emerging threats.

The most common types of cyberattacks are:

1. Phishing attacks deceive victims into revealing sensitive information through fake emails or websites.

2. Botnet attacks involve compromising multiple systems to carry out malicious activities, often for financial gain or disruption.

3. Malware attacks involve installing harmful software to gain unauthorized access, steal information, or damage systems, with examples including viruses, spyware, ransomware, and Trojans, each exploiting specific vulnerabilities.

4. SQL injection attacks exploit database vulnerabilities to gain unauthorized access, modify, or delete sensitive data, often bypassing authentication processes.

5. DDoS attacks overwhelm a target server with high traffic from multiple sources, often using botnets, to disrupt access to legitimate users. The primary goal of DDoS attacks is service disruption, usually for financial gain or to harm the target organization.

Cybersecurity in Aviation

CURRENT LANDSCAPE

The aviation industry has adopted advanced and more efficient digital technologies to improve operational efficiency, safety and passenger experience. This digital transformation has resulted in the development of highly connected systems that streamline every process: from in-flight services to air traffic management. The existing isolated and standalone systems have been replaced for a web of interconnected networks and devices, including IoT sensors, actuators, biometric readers, robotics and cloud applications, all requiring web connectivity (Gnatyuk, 2016) (Mills, 2014) (McCarthy, 2014).

With increased connectivity and digitalization of processes comes an expanded attack surface, and new and complex vulnerabilities emerge (Kagalwalla & Churi, 2019). Aircraft systems, in-flight entertainments, air traffic control and ground services are all linked to enhance coordination and service, but each of these interfaces poses a new entry point for malicious events.

Smart Airports: interconnected environments introduce vulnerabilities such as network attacks and malware due to hardware limitations or misconfigurations.

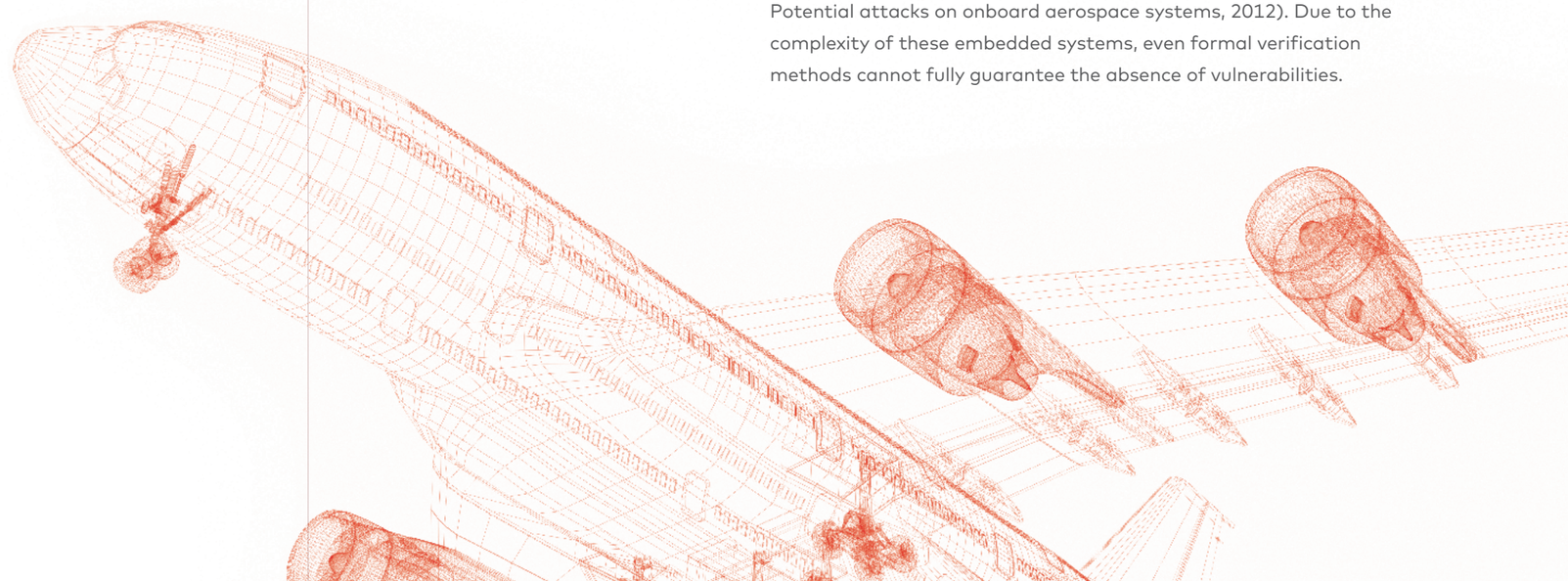
E-enabled aircraft: use of electronic data exchange and digital network connectivity might create attack surfaces for radio frequency jamming, impersonation and eavesdropping.

While navigation and other avionic systems are designed to be completely independent and isolated from external networks, making them less susceptible to corruption, certain aircraft systems remain vulnerable to intentional manipulation. Communication between aircraft and the ground can be intercepted and critical data can be wiped out, corrupted or stolen. This scenario exposes aviation to a range of risks, compromising not only operational safety but also passenger trust and service efficiency. The shift towards integrated digital solutions within the industry has boosted efficiency but has made cybersecurity a critical focus for aviation.

OVERVIEW OF AVIATION SYSTEMS STRUCTURE

The integration of technologies such as Internet of Things (IoT), Global Positioning System (GPS), open-source platforms, virtualization, and cloud computing, has become a cornerstone of modern aviation systems (Haass, Aviation and cybersecurity: opportunities for applied research, 2016). These innovations play a central role in streamlining operations, reducing costs, and enhancing inter-operational response times (Haass, Aviation and cybersecurity: opportunities for applied research, 2016). However, the integration of these technologies also introduces remote access capabilities, which inherently increase system vulnerabilities. As a result, aviation systems are inherently complex, and any disruption to their normal operations requires comprehensive expertise in both the broader aviation systems and the specific configurations of individual aircraft (Paganini, 2014).

Modern aviation systems rely on intricate layers of integrated software and hardware, often implemented through embedded systems (Papp, 2015) (Dessiatnikoff, Potential attacks on onboard aerospace systems, 2012). These avionics systems provide critical support to crew members and pilots, aiding in the safe operation of aircraft by delivering essential information on weather, positioning, and communications. Avionics, defined as the integration of aviation and electronics, encompasses the design, development, and operation of embedded systems in aircraft. These systems collect data, such as speed, direction, altitude and air temperature, through external sensors and route this data to other aircraft components via an avionics network (Smith B., 2006). Researchers further highlight that attacks on aerospace systems may exploit lower layers, including the operating system (OS) kernel, protection mechanisms, and context-switching processes (Dessiatnikoff, Potential attacks on onboard aerospace systems, 2012). Due to the complexity of these embedded systems, even formal verification methods cannot fully guarantee the absence of vulnerabilities.



GROWTH IN THREATS

Cyber incidents in aviation have become more frequent and costly, affecting airlines and airports worldwide. Notable incidents such as data breaches and ransomware attacks have led to operation downtime, flight delays, data theft, large financial losses and the possibility of national security implications.

According to EUROCONTROL, in 2023 ransomware was one of the two top threats alongside attacks against availability, costing companies approximately 5% of their annual revenue (EUROCONTROL, 2023). Also, in the first half of 2023, cyberattacks in the aviation industry increased by 24% worldwide and ransomware attacks on supply chain players in 2023 went up as much as 600% compared to 2022 (ACICE, 2024 May).

THREATS AND VULNERABILITIES

Threat actors can be categorized into several distinct types, each driven by unique motivations. The primary categories include i) financial gain (infliction of economic losses to stakeholders in the aviation industry), ii) defense of ideological or political ideas, iii) espionage, iv) instigation of violence or disruption of social structures and v) geopolitical advantage (conducted by state-sponsored cyber-warriors to further strategic interests of supporting nations). These varied motivations reflect the complex landscape of cyber threats, where attacks may aim to disrupt operations, exfiltrate information, or serve larger political and financial objectives.

Appendix A (Ukwandu, et al., 2022) presents the 27 major cyberattacks in civil aviation between 2003 and 2021, acknowledging the possibility of additional incidents that may have been excluded due to underreporting or omission. The analysis of potential vulnerabilities and possible entry points for attackers is crucial to guarantee the security of systems. Supply chain and third-party providers, unsupported or unmaintained software, mobile devices, reservation systems, flight history servers, ticket booking portals, flight management systems and cabin crew devices might constitute potential backdoors for attackers. A real-world example of a security vulnerability occurred when an attacker gained access to the in-flight entertainment system by connecting a modified Cat6 cable to his laptop (Zetter, 2015). Moreover, other systems within the airplane's network could potentially be compromised in a similar way (Freiherr, 2021).

1. DDoS Attack on LOT Polish Airlines (2015)
In 2015, a DDoS attack breached LOT Polish Airlines' information technology system, compromising their ground computers for five hours. As a result, the airline was unable to issue flight plans for outbound flights from its central hub, leading to the cancellation of around 20 flights.

2. Cyberattack on SITA, a Global IT Provider for the Aviation Industry (2021)
In 2021, a cyberattack on SITA, a global IT provider for the aviation industry, resulted in a significant passenger data breach. Air India was one of the affected airlines, with the personal details of approximately 4.5 million customers being compromised

3. Accidental Data Wipe on Airbus Engines (2015)
In 2015, during maintenance at Airbus facilities, the torque calibration parameter data was accidentally wiped on three engines. Under the aircraft's design, the first warning was only given when the plane was 120 meters in the air, causing the plane to crash. Although this incident was unintentional, it highlights an unidentified vulnerability that could have been exploited by hackers to harm the isolated avionic systems.

Regulatory Landscape

EXISTING STANDARDS – CIVIL AVIATION

In aviation, cybersecurity standards are vital for ensuring the safety and security of aircraft systems. The DO-326A/ED-202A Set, published jointly by RTCA (US) and EUROCAE (Europe) respectively, forms the foundation of the regulatory landscape, guiding cybersecurity implementation across civil aviation platforms.

The set was based on the de-facto industry standards ARP4754 and DO-178, but it relies on different key assumptions: i) covers security aspects not only related to software (like hardware, guidelines, procedures, among others), and ii) takes into consideration harmful and intentional actions as events that could threaten the airworthiness security of the aircraft. It establishes the Airworthiness Security Process (AWSP) to guarantee that, when subjected to unauthorized interaction, the aircraft will remain in a condition of safe operation. This is achieved by 1) an exhaustive security risk assessment and 2) certification activities to validate that these risks are acceptable per the defined criteria.

The DO-326A/ED-202A (revised version on airworthiness security process specification) document was released in 2014 and applies to aircraft manufacturers, suppliers and others involved in aircraft design and focuses on identifying, assessing and mitigating cyber risks during design and operational phases. Although it is not enforced by law, it is essential for compliance with aviation authorities, and it covers the "what" of the certification process. The DO-356A/ED-203A revised document (Airworthiness security methods and considerations) involves threat assessment and risk management, covering the "how" of the certification process.

Core Guidance

- **DO-326A/ED-202A:** guidelines for establishing a security process to address cyber threats that could affect the airworthiness of an aircraft
- **DO-356A/ED-203A:** methodologies and guidance for meeting the security objectives laid out in DO-326A/ED-202A

In-service Guidance

- **DO-355/ED-204:** guidance for the operation and maintenance of aircraft
- **DO-392/ED-206:** security event management for various stakeholders in the aviation environment

Top-Level Documents

- **DO-391/ED-201:** framework for linking the various security standards for aviation security together to support all stakeholders
- **Introduction of an Information Security Management System**

Gound Systems Standard

- **DO-393/ED-205A:** provides a process to assess the extent to which the Air Traffic Management and Air Navigation Services systems are appropriately secure for use in aviation

From a higher-level standpoint, breaches in information can lead to safety consequences, making it essential to impose robust information security requirements that limit their impact on acceptable levels of aviation safety. The Part-IS (Part Information Security) is the latest EASA regulation to identify and manage information security risks with potential impact on aviation safety (refers to the two EU regulations Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation 2022/1645). It addresses the challenge of cyber threats and information vulnerabilities in the industry.

One of the key elements of the established framework is the implementation of an ISMS — Information Security Management System. Contrary to the one specified in ISO 27001 (general ISMS applicable to a wide range of companies), it is specifically applicable to companies subject to strict aviation requirements.

FUTURE REGULATIONS AND EXPECTED UPDATES

The aviation industry is continually updating cybersecurity standards to address emerging threats and adapt to evolving technologies. The following Aviation Industry-Specific Cybersecurity Standards are expected to be released after significant revision:

- **DO-326B/ED-202B:** improvement on change impact analysis related to information security of embedded systems; guidance for authority involvement on the compliance demonstration; guidance on how to facilitate implementation of security update on certified products.
- **DO-392A/ED-206A:** Revised guidance on managing and responding to security events within aviation systems.

Part-IS Compliance Framework

IS Management System

- Preservation of confidentiality, integrity, authenticity and availability of network and information systems

Continuous Improvement

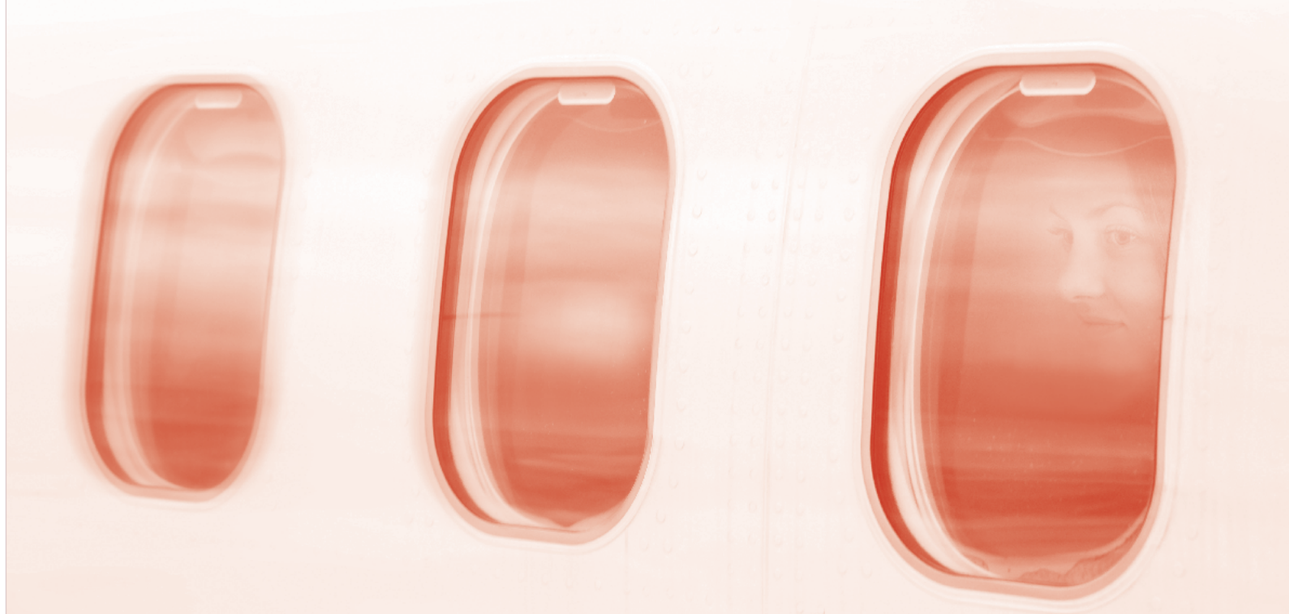
- Technical and organisational systems
- Documented proceses, roles and responsabilities

Reporting System

- Internal and external reporting
- Foster collaboration across stakeholders and accountability

Management Mechanism

- Detect, manage, respond and mitigate cyber and information security risks



Mitigation Strategies

BEST PRACTICES

Considering the increasing threat landscape, cybersecurity emerges as an essential solution to protect aviation's critical infrastructures. Implementing rigorous digital security measures and applying a well-structured cybersecurity framework makes it possible to mitigate risks and ensure that aviation continues to operate safely, efficiently, and reliably, maintaining passenger trust and industry stability.

Technologies such as micro-segmentation (Monteagudo, 2020) and deception (Bellekens, 2019) are currently discussed strategies in cyber-defense, particularly within critical infrastructures like aviation. Micro-segmentation involves dividing networks into smaller, isolated segments, each with its own access controls. This approach ensures that any cyberattack, or data breach, is contained within a specific segment, preventing it from spreading across the entire network. On the other hand, deception technology creates false environments within the system to detect cyber threats early. By luring attackers into fake networks or systems, it helps identify intrusions and malicious activities before they can cause significant damage.

Mitigation strategies are grounded in the importance of a thorough risk assessment process, as stated in the applicable regulations and standards. This process is essential for defining threat scenarios, characterizing security measures and evaluating the risk of each case having a safety effect on the system/aircraft assets. By integrating risk assessments into the overall safety and security framework, organizations can prioritize mitigation measures to address the most critical risks effectively. This structured approach ensures that safety objectives are met, supporting the resilience and reliability of aviation systems while maintaining compliance with regulatory requirements.

On a more holistic approach to cybersecurity, measures such as cybersecurity training and awareness, security by design and collaboration across the industry have been discussed frequently in the community. The goal is to identify and mitigate security risks as early as possible in the development process, fostering a culture of cooperation.

One of the practices adopted by Critical Software in this regard is secure coding. Security requirements such as data protection and potential system threats are outlined and discussed before development. During the development phase, developers follow secure coding principles such as i) input validation to prevent malicious data entry, ii) implementation of strong authentication, and iii) careful error handling to avoid exposing sensitive information. Regular code reviews and security testing are conducted to detect and resolve vulnerabilities, ensuring that the code is robust and resilient against potential attacks before deployment.

Furthermore, it enables the identification of vulnerabilities in the libraries and components incorporated into the software. As discussed above, while some avionics systems are completely isolated where every part is developed from scratch, eliminating the need for external imports, there are other systems with incorporated dependencies that may impact the safety of the aircraft. These systems benefit particularly from a secure coding approach to ensure that potential vulnerabilities are identified and mitigated effectively.

THE RUNSAFE SECURITY PLATFORM

In addition to risk assessments and following Secure by Design and secure coding best practices, Critical Software partners with RunSafe to further protect critical embedded systems in the aviation industry. By deploying solutions like Runtime Exploit Prevention, the industry can protect aircraft software in real time.

The RunSafe Security Platform provides vulnerability identification, runtime code protection, and passive monitoring to protect military and commercial avionics systems, aviation controls, and ancillary systems. Specifically, RunSafe provides build-time Software Bill of Materials (SBOMs) for full visibility into software, automated vulnerability identification and prioritization, and continuous protection for aviation systems through RunSafe's patented Load-time Function Randomization process.

By generating comprehensive SBOMs and applying runtime protections, RunSafe is able to protect aviation systems from memory-based vulnerabilities, which have the most known exploits targeting them as compared to any other class of vulnerability. Malicious actors exploit memory safety vulnerabilities to execute arbitrary code, compromise sensitive data, or cause system crashes.

For example, if an attacker successfully exploits a buffer overflow vulnerability, a type of memory safety issue, and injects into the software malicious commands, an aircraft with human lives on board could become compromised, making critical components necessary for flight and control non-operational. Even communications with ground control could be jeopardized.

RunSafe's software memory protection reduces the potential attack surface of aviation systems, preventing cybercriminals from exploiting both known memory vulnerabilities and future zero days.

By implementing RunSafe's advanced security measures, aviation vendors are able to protect embedded systems in avionics that are critical to the safe and reliable operation of aircraft without rewriting code.

Conclusion

The increasing reliance on interconnected technologies in aviation has significantly expanded the industry's attack surface, making cybersecurity a critical priority. From safeguarding avionics systems to protecting passenger data, robust cybersecurity measures are essential to ensuring the safety, efficiency, and trustworthiness of aviation operations.

This white paper has highlighted the evolving threat landscape, regulatory frameworks, and effective mitigation strategies. Moreover, technologies like those provided by RunSafe exemplify innovative approaches to address vulnerabilities and enhance resilience in aviation systems.

As the aviation sector continues to innovate, a comprehensive and adaptive approach to cybersecurity will remain indispensable to counter emerging threats and maintain operational integrity in a rapidly evolving digital landscape.

To find out more about our work, please get in touch: aviation@criticalsoftware.com

Appendix

Appendix A – Cyberattacks in Civil Aviation (2003-2021)

Class	Ref	Year	Incident	Source	Location	Description
C	26	2009	Malicious hacking attack	OTR	USA	A malicious hacking attack on FAA's computer, through which hackers gained access to personal information of 48,000 current and former FAA employees.
C	27	2013	Malware attack	OTR	Istanbul, Turkey	Shutting down of passport control system at the departure terminals of Istanbul Ataturk and Sabiha Gokcen airports due to a malware attack, leading to the delay of many flights.
C	28	2013	Hacking and phishing attacks	OTR	USA	Malicious hacking and phishing attacks that targeted about 75 airports. These major cyberattacks were alleged to have been carried out by an undisclosed nation-state that sought to breach US commercial aviation networks.
A	29	2015	DDoS attack	OTR	Poland	A Distributed Denial-of-Service (DDoS) attack by cybercriminals that affected LOT Polish Airlines flight-plan IT Network systems at the Warsaw Chopin airport. The attack rendered LOT's system computers unable to send flight plans to the aircraft, thus grounding at least 10 flights, leaving about 1400 passengers stranded.
I	30	2016	Hacking and phishing attacks	OTR	Vietnam	The defacement of a website belonging to Vietnam airlines and flight information screens at Ho Chi Minh City and the capital, Hanoi, displaying messages supportive of China's maritime claims in the South China Sea by Pro-Beijing hackers.
A	31	2016	Cyber-Attack	OTR	Boryspil, Ukraine	A malware attack was detected in a computer in the IT network of Kyiv's main airport, which includes the airport's air traffic control system.
A	30	2017	Human error	OTR	United Kingdom	British flag-carrier computer systems failure caused by disconnection and re-connection of the data-center power supply by a contracted engineer. This accident left about 75,000 passengers of British Airways stranded.
C	32	2018	Data breach	OTR	Hong Kong	Cathay Pacific Airways data breach of about 9.4 million customers' personal identifiable information.
C	33	2018	Data breach	OTR	United Kingdom	British Airways Data breach of about 380,000 customers'
C	36	2018	Mobile app data breach	OTR	Air Canada, Canada	Air Canada reported a mobile app data breach affecting
C	37	2018	Data breach	OTR	Washington DC, USA	Data breach on a NASA server that led to possible compromise of stored personally identifiable information (PII) of employees on 23 October 2018.
C	38	2018	Ransomware attack	OTR	Chicago, USA	Boeing was hit by the WannaCry computer virus, but the attack was reported to have minimal damage to the company's internal systems.
A	20	2018	Cyber-Attack	TP	Sweden	Cyber-attack launched by Russian APT group (APT28) that blocked Sweden's air traffic control capabilities, grounding hundreds of flights over a 5-day period.
A	39	2019	Bot attacks	OTR	Ben Gurion Airport, Israel	About 3 million bots attacks were blocked in a day by Israel's airport authority, as they attempted to breach airport systems.
C	40	2019	Cyber Incident	OTR	Toulouse, France	A cyber incident that resulted in unauthorized access to Airbus "Commercial Aircraft business" information systems. There was no known impact according to the report on Airbus' commercial operations.
C	41	2019	Ransomware attack	OTR	Albany, USA	Albany International Airport experienced a ransomware attack on Christmas of 2019. The attackers successfully encrypted the entire database of the airport forcing the authorities to pay a ransom in exchange of the decryption key to a threat actor
C	42	2019	Crypto mining Malware infection	OTR	Europe	Cyberbit researchers discovered through their security software, known as EDR, a network infection of more than 50% of the European airport workstations by a cryptocurrency mining malware.
C	43	2019	Phishing attack	OTR	New Zealand	A phishing attack targeted at Air New Zealand Airpoints customers. This attack compromised the personal information of approximately 112,000 customers, with names, details and Airpoints numbers among the data exposed.
C	44	2020	Ransomware attack	OTR	Denver, USA	A cyber-incident that involved the attacker accessing and stealing company data, which were later leaked online.
C	45	2020	Ransomware attack	OTR	San Antonio, USA	Data breach suffered by ST Engineering's aerospace subsidiary in the USA that later led to a ransomware
I	46	2021	Software Error	OTR	Birmingham, United Kingdom	A software error in the IT system that could not recognize mass discrepancies between load sheet and the flight plan, leading to the aircraft having 1606 kg more take-off mass than required.

References

Bellekens, X. a. (2019). From cyber-security deception to manipulation and gratification through gamification. HCI for Cybersecurity, Privacy and Trust: First International Conference (pp. 99-114). Springer.

Cybersecurity Threats to Aviation. (2023, April). Retrieved from https://aviationweek.com/air-transport/airlines-lessors/cybersecurity-threats-aviation-bolstered-efficiency-geopolitics

David, A. (n.d.). DO-391/ED-201. Afuzion.

Deloitte, & Word Economic Forum. (2021). Pathways Towards a Cyber Resilient Aviation Industry. Retrieved from https://www.weforum.org/publications/pathways-towards-a-cyber-resilient-aviation-industry/

Dessiatnikoff, A. a. (2012). Potential attacks on onboard aerospace systems. IEEE Security & Privacy, 71-74.

EUROCAE. (2019). ED-205. Retrieved from https://www.eurocae.net/news/posts/2019/march/ed-205-process-standard-for-security-certification-and-declaration-of-atm-ans-ground-systems/

EUROCONTROL. (2023, February). EUROCONTROL Data Snapshot #39 on ransomware groups targeting aviation's supply chain. Retrieved from https://www.eurocontrol.int/publication/eurocontrol-data-snapshot39-ransomware-groups-targeting-aviations-supply-chain

ACICE (2024, May) ADMM Cybersecurity and Information Centre of Excellence: Update On The Cyber Domain - Cyber Threats in Aviation. Retrieved from https://www.acice-asean.org/files/cybersecurity%20centre%20reports/may_24_cyber.pdf

Freiherr, G. (2021). Will Your Airliner Get Hacked?

Gnatyuk, S. (2016). Critical aviation information systems cybersecurity. Meeting security challenges through data analytics and decision support (pp. 308-316). IOS Press.

Haass, J. a. (2016). Aviation and cybersecurity: opportunities for applied research. Tr News, 39.

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

LTD, R. (n.d.). EASA Part-IS Regulation. Retrieved from https://part-is.eu/regulation/

McCarthy, C. a. (2014). National institute of standards and technology (nist) cybersecurity risk management framework applied to modern vehicles. United States. Department of Transportation. National Highway Traffic Safety.

Mills, S. a. (2014). Cybersecurity challenges for program managers. Defense AT\&L, 41-43.

Monteagudo, J. (2020). Aviation Cybersecurity - High Level Analysis, Major Challenges and Where the Industry is Heading. Smartrev Cybersec.

Paganini, P. (2014). Cyberthreats against the aviation industry. Retrieved from Infosec. Available at: http://resources. infosecinstitute. com/cyber-threats

Papp, D. a. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 2015 13th Annual Conference on Privacy, Security and Trust (PST) (pp. 145-152). ieee.

Radio Technical Commission for Aeronautics. (n.d.). Security - RTCA. Retrieved from https://www.rtca.org/security/

Rupprich, A., & Schumacher, W. (2024, October). Part-Is: The 7 Most Important Questions.

SITA. (2021, March). SITA Statement about security incident. Retrieved from https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/

Smith, B. (2006, September). System and method for data collection in an avionics network. Google Patents.

Smith, D. (n.d.). Staying Cybersecure in the aerospace sector. Retrieved from https://www.aerospacetestinginternational.com/features/staying-cybersecure-in-the-aerospace-sector.html

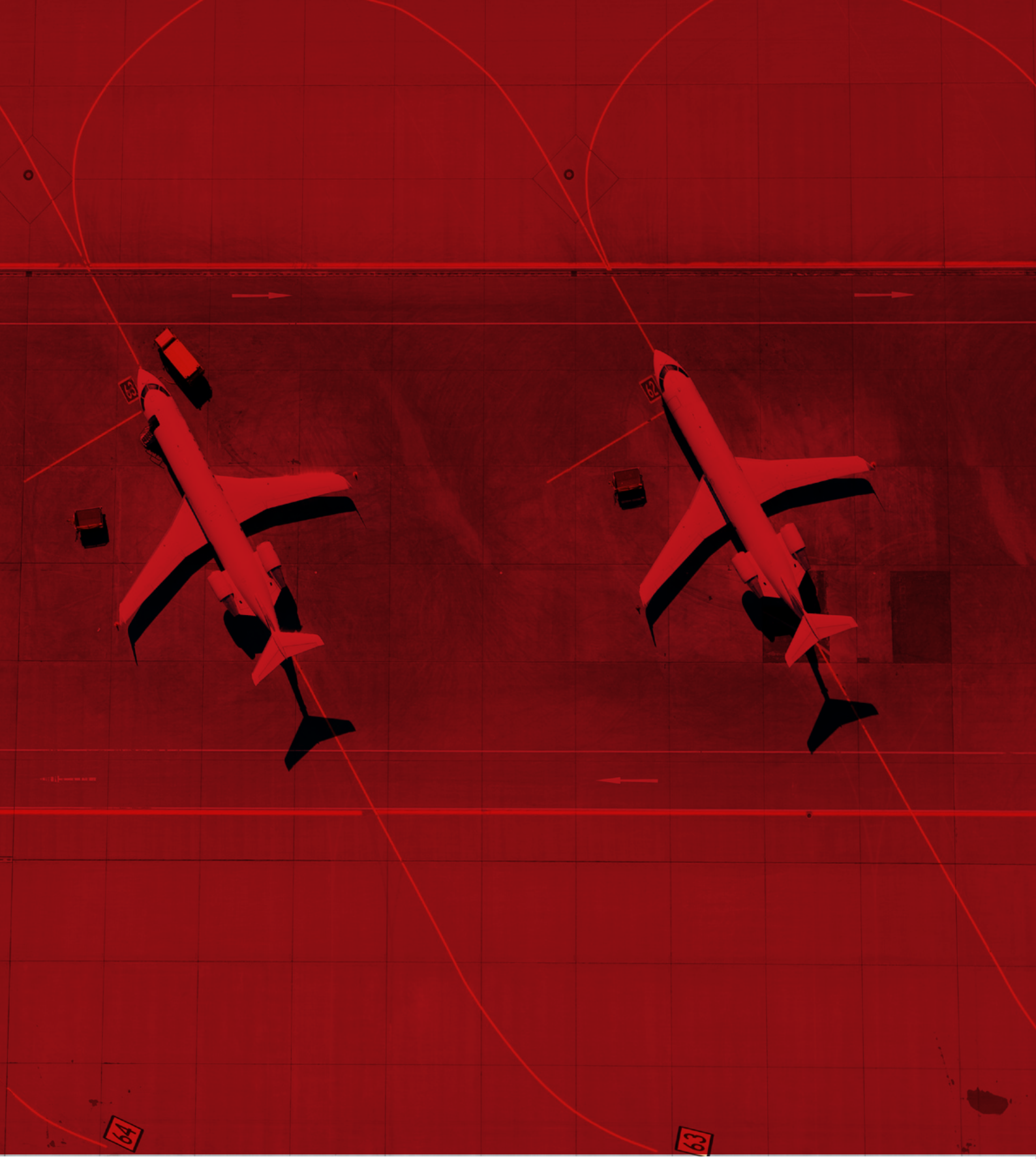
Sudar, K. M. (2020). Analysis of cyberattacks and its detection mechanisms. 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) (pp. 12-16). IEEE.

Ukwandu, E., Ben-Farah, M., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends.

Wadho, S. A. (2023). Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review. VAWKUM Transactions on Computer Sciences, 295-305.

Werthwein, M., Brunner, M., & Annighoefer, B. (2023). A Concept Enabling Cybersecurity for a Self-Adaptive Avionics Platform With Respect to RTCA DO-326 And RTCA DO-356. 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference, 1-10.

Zetter, K. (2015). Zetter, K. Feds Say that Banned Researcher Commandeered a Plane. Retrieved from: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.



We are CMMI Maturity Level 5 rated.

For a list of our certifications & standards
visit our website.

criticalsoftware.com
info@criticalsoftware.com