SKYGRID

Closing the Gap: Addressing the Need for Comprehensive Cybersecurity in Advanced Air Mobility and Autonomous Aviation

White Paper

State of Cybersecurity Standards in Aviation

The aviation industry's approach to cybersecurity is primarily driven by standards and regulations set forth by regulatory bodies, including the Federal Aviation Administration (FAA), the International Civil Aviation Organization (ICAO), the European Union Aviation Safety Agency (EASA), and others. These organizations have laid the foundation for ensuring the safety and security of traditional, manned aviation operations.

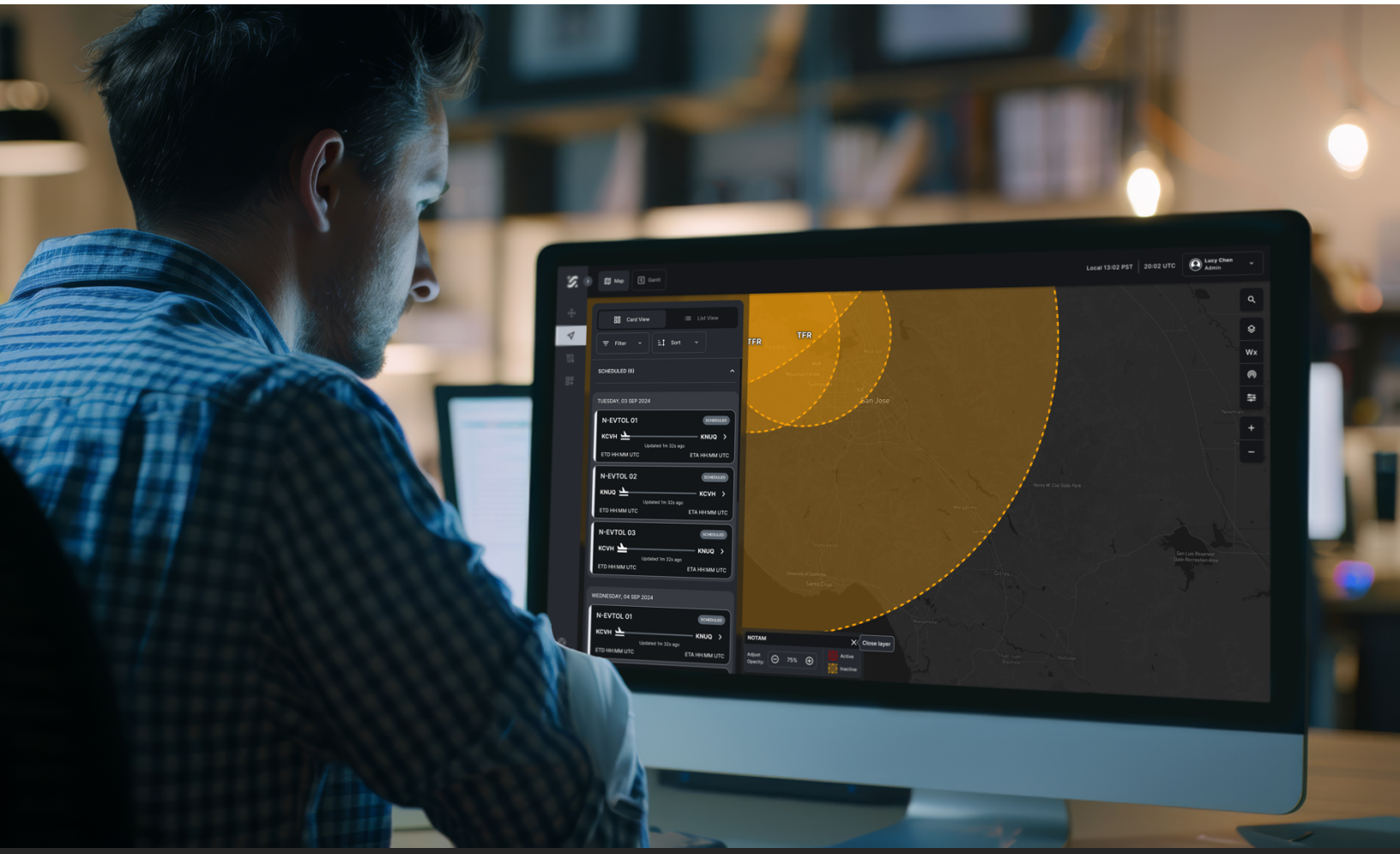
The FAA, for example, has introduced various cybersecurity requirements within its regulatory framework. These standards primarily concern conventional, onboard aircraft systems. Similarly, ICAO and EASA have released guidelines and standards, such as ICAO's Cybersecurity Framework for civil aviation, focusing again on the established aviation ecosystem.

However, existing standards and regulations reveal significant gaps when applied to emerging aviation technologies like Advanced Air Mobility (AAM) and autonomous flight. Traditional aviation cybersecurity frameworks, including the DO-326A standard, have limitations in covering the new types of operational models and technological infrastructure brought forward by AAM.

For example, current standards generally do not address the cybersecurity needs of highly automated and autonomous systems or provide guidance on end-to-end security in distributed systems and networks. This gap becomes critical as these new aviation technologies and operations increasingly depend on distributed and connected digital infrastructures for navigation, communication, and data processing, all highly susceptible to cyber threats.

Existing regulations also lack specific guidance for managing the cybersecurity risks of one-to-many operations in autonomous systems, where a single operator may control, supervise, or dispatch multiple vehicles. Furthermore, current frameworks do not adequately cover the complexity and scale of cybersecurity risks that come with cloud-based data storage, real-time communication systems, and remote management capabilities.

As a result, stakeholders in AAM and autonomous aviation are left with limited options for ensuring the cybersecurity of these novel systems. This creates an urgent need for a robust and adaptive cybersecurity framework that can meet the needs of the evolving advanced aviation landscape.



Emergence of Third-Party Service Providers (TSPs)

Third-party service providers (TSPs) are increasingly vital to the aviation ecosystem, particularly for enabling AAM and autonomous flight operations. TSPs provide essential digital services such as communication, navigation, and surveillance (CNS) functions, as well as situational awareness, decision support, and data distribution for scalable and efficient operations.

These services are delivered through user interfaces and APIs that offer planning, alerting, and advisory capabilities, enabling seamless operation in today's complex airspace systems.

As a TSP, the SkyGrid system will provide AAM operators flying both crewed and uncrewed missions with a detailed digital representation of their operating environment. This includes pre-flight and in-flight situational awareness tools to enhance safety and decision-making efficiency.

Challenges with Current Standards for TSP Requirements

TSPs operate in highly interconnected environments, facilitating real-time data exchange between ground control, cloud-based systems, and airborne assets. This level of integration introduces new cybersecurity risks that are not fully accounted for by standards like DO-326A. The SkyGrid Cybersecurity team analyzed multiple EUROCAE, RTCA, and ASTM standards to find that these standards are suitable for defining security controls in traditional aircraft systems where the physical enclosure is considered a threat boundary and physical security is key. TSPs however must consider additional threat models, actors, and interconnected architectures. Systems must also account for jamming and spoofing on the ground in addition to the cyber control framework.

We find that the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and the International Organization for Standardization (ISO) 27001 Information Security Management offer a more robust, comprehensive, and adaptable model for implementing cybersecurity measures in the rapidly evolving domain led by TSP's. These frameworks support a risk-driven approach to cyber and cyber-physical threats such as jamming and spoofing.

Securing communication channels across multiple entities (e.g., ground operators and autonomous vehicles) requires advanced encryption protocols, dynamic authentication measures, and real-time threat detection. These challenges are heightened by the dependency on TSPs for real-time decision-making data, where a reduction in system integrity or availability could directly impact safety. Updated standards are needed to address these gaps and provide an end-to-end cybersecurity framework tailored to address the complex demands of TSP-reliant ecosystems.

Cyber Threats Facing TSPs Supporting AAM and Autonomous Aviation

The shift towards autonomous aviation and AAM brings a new spectrum of cybersecurity challenges, particularly for third-party service providers. Autonomous operations increase the risk and consequences of cyberattacks on communication, navigation, and control systems, particularly in one-to-many operations where a single operator or digital service provider oversees or supports multiple vehicles. In these environments, TSPs often serve as the backbone for data management and connectivity, making them attractive targets for cyber threats.

A significant risk stems from the connectivity required between autonomous vehicles and ground-based systems. For example, a cyberattack on a TSP's network could disrupt the data flow necessary for real-time situational awareness, potentially resulting in loss of separation, collisions, encounters with hazardous weather, or other operational hazards. An example of a potential attack could involve a hacker compromising the TSP's data server and altering navigation data sent to an autonomous vehicle. Such interference could mislead the vehicle's automated systems and cause it to veer off its intended route or violate airspace regulations, with potentially catastrophic outcomes.

Furthermore, cloud-based functions that underpin AAM add another layer of vulnerability that cannot be overlooked. Many TSPs rely on cloud storage and processing to manage critical flight data, exposing them, via their infrastructure, to cyber threats like data breaches, ransomware attacks, and denial-of-service incidents. Moreover, the integration of safety-critical functions with remote systems amplifies these risks, as these systems must maintain a secure and uninterrupted flow of data to guarantee operational safety. These vulnerabilities must be addressed to ensure the reliability and safety of autonomous operations.

Given these increased risks, it is essential to prioritize cybersecurity for TSPs supporting AAM and autonomous operations. This prioritization distinguishes the approach of forward-thinking organizations, who fully recognize that solving these vulnerabilities requires a heightened focus on cyber resilience across connected systems and networks.

Achieving TSP Cybersecurity

After assessing all existing aviation cybersecurity standards, the National Institute of Standards and Technology (NIST) cybersecurity framework has emerged as a robust solution for addressing TSP cybersecurity. NIST provides a comprehensive, adaptable framework focused on flexibility, risk management, and best practices tailored to high-risk industries, making it particularly effective for the complex cybersecurity requirements of TSPs.

Utilizing its five core functions—Identify, Protect, Detect, Respond, and Recover—the NIST framework supports continuous monitoring and real-time threat detection, which are essential for maintaining security within the interconnected aviation sector. This risk-based approach is compatible with aviation standards.

Comprehensive Approach

Unlike traditional aviation standards like DO-326A, which are narrowly focused on specific onboard components, NIST's framework is adaptable across different hosting environments and architectures. It allows TSPs to implement a multi-layered approach to cybersecurity, addressing a wide range of risks from data protection and identity management to incident response and recovery.

Corporate and Product Cybersecurity

The NIST framework covers both organizational practices and technical controls, helping TSPs secure their infrastructure at every level. It provides guidance on implementing cybersecurity across corporate processes and product development, ensuring that the organization's cybersecurity policies align with the systems that they develop and manage. By adopting the NIST framework, TSPs can unify their security strategies across corporate governance and product development, strengthening their defense against cyber threats.

Industry Best Practices

The NIST framework draws from industry best practices beyond aviation, allowing TSPs to benefit from cybersecurity advancements across sectors, including healthcare, finance, defense, and critical infrastructure. By leveraging NIST's comprehensive standards—proven effective in these high-risk industries—TSPs can establish resilient cybersecurity measures that adapt to changing threats, ensuring they meet the rigorous security needs of complex AAM and autonomous flight operations.

Enabling Automation and Autonomous Trust

For TSPs like SkyGrid, a well-structured cybersecurity framework not only ensures the security of their digital infrastructure but also instills trust in the AAM and autonomous aviation ecosystem. By employing the NIST cybersecurity framework, SkyGrid can establish a resilient digital foundation that minimizes risk, protects critical data, and enables safe and reliable AAM operations.

SkyGrid's choice of NIST supports enhanced automation and autonomy within aviation, ensuring that autonomous systems can operate securely with minimal human intervention. Furthermore, SkyGrid's use of a cross-sector cybersecurity framework allows it to innovate on learnings from adjacent, safety-critical industries and address the expanded needs of cloud-based distributed TSPs.

Secure TSP systems are essential for building trust in automated and autonomous aircraft operations. By adopting strong cybersecurity measures, TSPs empower these technologies to achieve greater autonomy, reducing the necessity for human oversight while maintaining rigorous safety and compliance with aviation standards. What we learn in the context of TSP for AAM can also be applied to other segments of increasingly connected and digitized aviation. Embracing a thorough and proactive approach to cybersecurity allows TSPs like SkyGrid to help enhance the safety and efficiency of AAM operations.

Industry leaders and regulators need to come together to establish robust cybersecurity standards. We call on all stakeholders to actively validate the NIST Cybersecurity Framework (CSF) as a foundational blueprint. By doing so, we can collectively fortify our security measures and ensure the successful, safe evolution of advanced aviation and digital airspace.

SKYGRID

For more information about SkyGrid, visit skygrid.com

Follow us at: