Cyber Security Technical Panel
Technical Operations Panel Report

Victor Murray, CISSP
Chair, Cyber Security Technical Panel

AESS Board of Governors Meeting – Fall 2025
10-11 October 2025
Krakow, Poland

Cyber Security Panel Mission and Objectives

MISSION

- **Risk and Threat Tracking.** Develop and maintain a comprehensive understanding of the cybersecurity threats and risks to the aerospace and electronics sectors.
- **Cybersecurity Best Practices.** Promote and support the adoption of cybersecurity best practices throughout the IEEE AESS.
- **Stakeholder Collaboration.** Coordinate and collaborate with other stakeholders to ensure a harmonized approach to cybersecurity.

OBJECTIVES

- **Risk and Threat Tracking.** To understand the cybersecurity threats and risks that affect the AESS sectors. This will be accomplished by developing and maintaining a comprehensive knowledge base of cybersecurity vulnerabilities and threats that can affect the sectors of interest and their respective assets. The threats and vulnerabilities will be prioritized to identify the most critical cybersecurity vulnerabilities.
- **Mitigations.** To develop recommended mitigation strategies and controls for the ecosystem of each sector that can prevent, detect, respond to, and recover from cybersecurity incidents.
- **Cybersecurity Best Practices.** To promote and support the adoption of cybersecurity best practices throughout the AESS to improve its cybersecurity posture.
- **Training.** Provide cybersecurity training and education to associated industry personnel to equip them with the skills and knowledge to deal with cybersecurity incidents. This will be accomplished by papers and publications in various industry and cybersecurity conferences, magazines, and journals. In addition, distinguished lectures will be prepared by the Panel member and offered to IEEE member organizations, Local Chapters and through virtual media.
- **Awareness**. To enhance the cybersecurity awareness and knowledge of AESS industry personnel to enable them to detect and respond to cybersecurity incidents.
- **Collaboration.** To collaborate with other stakeholders to ensure a coordinated and comprehensive approach to AESS cybersecurity that aligns with the underlying sector's needs and priorities.

Cyber Security Panel Summary of Activities

- 23 members and growing!
- AWARDED - Request for challenge problems: AI in Cyber Security
  - In collaboration with Avionics Systems and Glue Technologies for Space Systems
  - Awarded Proposal: Federated AI for Resilient Avionics and Drone Operations by Intelligent Fusion Technology
  - 9 proposals received.
- Education, Research and Innovation
- Conference Contributions and Publications

Federated AI for Resilient Avionics and Drone Operations

Abstract

The rapid integration of digital avionics and autonomous drone operations into modern aerospace systems has significantly expanded the cyber-attack surface, exposing critical functions such as GPS navigation, Automatic Dependent Surveillance – Broadcast (ADS-B) communications, and control links to spoofing, jamming, injection, and adversarial manipulation. Current anomaly detection models deployed in aircraft and drones operate in isolation and cannot adapt quickly to novel or distributed threats. To address this gap, we propose Drone Resilience Integrated Flight Test (DRIFT) for Federated AI for Resilient and Reliable Operating Avionics Drones (FAIR-ROAD) Operations as the IEEE AESS cybersecurity challenge problem. The objective is to develop a simulation-based testbed where multiple aircraft and drones collaboratively train anomaly detection models using federated learning (FL). By sharing model updates rather than raw data, participants can collectively learn from diverse cyber observations while preserving privacy and operational constraints. The central challenge is to ensure that the federated global model remains resilient against poisoning attacks, constrained bandwidth and compute resources, and dynamic mission conditions. The testbed will include attack scenarios (e.g., GPS spoofing, ADS-B injection, model poisoning) and provide well-defined performance metrics (detection accuracy, robustness, latency, and mission continuity) to evaluate competing solutions. The deliverables include a software environment, documented evaluation framework, and baseline AI models, to enable the research community further to enhance AI/ML-based defenses for aerospace systems. By fostering multiple solution approaches, it will drive progress toward scalable, distributed, and resilient cyber defense in aviation and drone operations.

Education, Research, and Innovation

- Post-Quantum Cryptography
- Applying Zero-Trust to Avionics
- Risk Assessment
- Artificial Intelligence
- Hosting Technical Presentations

Conference Contributions and Publications

- Digital Avionics Systems Conference (DASC)
  - Best Paper Award: Model-Based Avionics Cybersecurity Framework for Identification of Risk and Evaluation
  - Panel Discussion on AI/ML in Cybersecurity
  - Paper and Presentation Submission on Zero Trust Architecture for Avionics
  - Paper and Presentation on Contemporary Directions in Cybersecurity Avionics Risk Analysis
- Integrated Communications, Navigation, and Surveillance (ICNS)
  - Towards Continuous Security Assessment: Integrating Model-Based Risk Assessment and Large Language Models
- International Carnahan Conference on Security Technology (ICCST)
  - Planning Committee
  - Post Quantum Cryptography Workshop
  - Panel Discussion on AI/ML in Cybersecurity
  - Keynote Speakers

Cyber Security Panel - Future Plans

- Magazine Article on Risk Assessment
- Special Publication on AI in Cyber Security
- Support DASC, ICCST, ICSN conferences
  - Panel Discussions
  - Publications
  - Keynotes
  - Workshops
- Phase 2: Request for Challenge Problem Proposals – AI in Cyber
- Technical Presentations and Training to Raise Cyber Awareness: Cybersecurity Best Practices