Cyber Security Panel
Technical Operations Panel
Semi-Annual Report

Victor Murray, CISSP; Jeff Chavis
Chair, Cyber Security Panel

AESS Board of Governors Meeting – Spring 2026
15-16 May 2026
Phoenix, AZ, USA

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

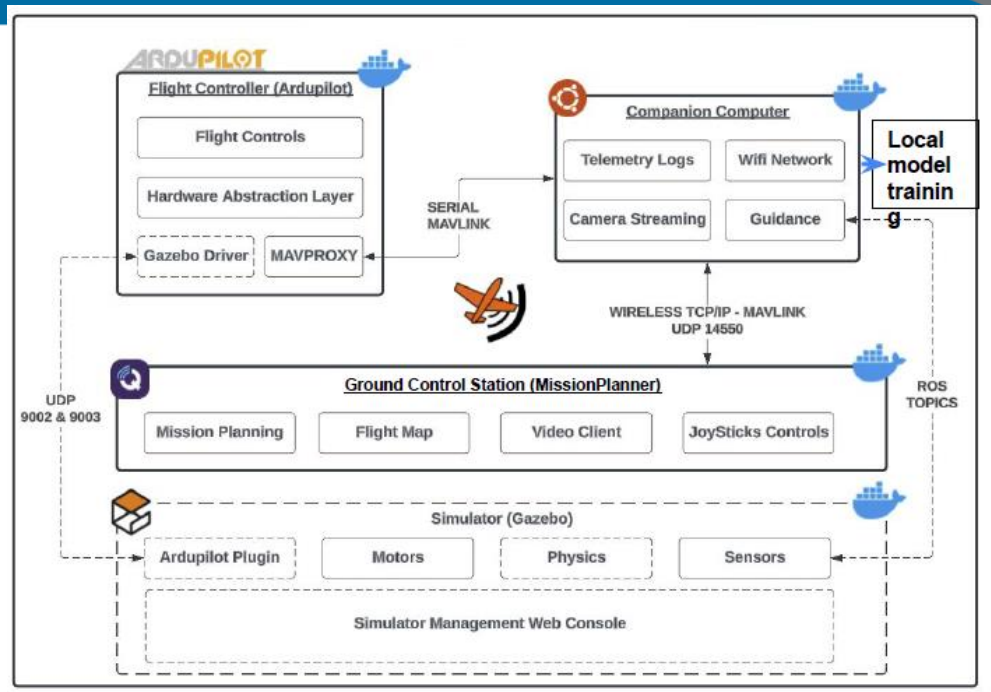
- Seven (7) new members nominated and confirmed to join Cyber Panel!
- Challenge problem definition: Federated AI to Secure Drone Networks
- Request for challenge problem solutions approved!
- AESS Special Publication Magazine Article
- Space Standards Collaboration
- Lots of Papers, Conferences, and Education
- DASC Best Cyber Paper!

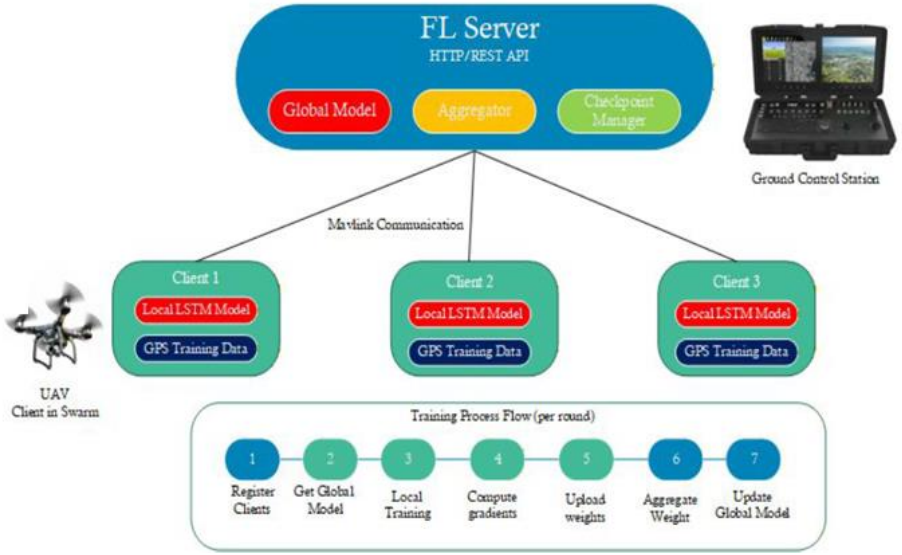
Federated AI for Cyber-Resilient Avionics/Drones

- Grant of $25K. Nine (9) Proposals submitted.
- Cyber Pane Technical Oversight
- Incredible Technical Work!

- AESS Tech Panel Collaboration:
  - Avionics
  - Glue Tech for Space Systems
  - Cyber Security

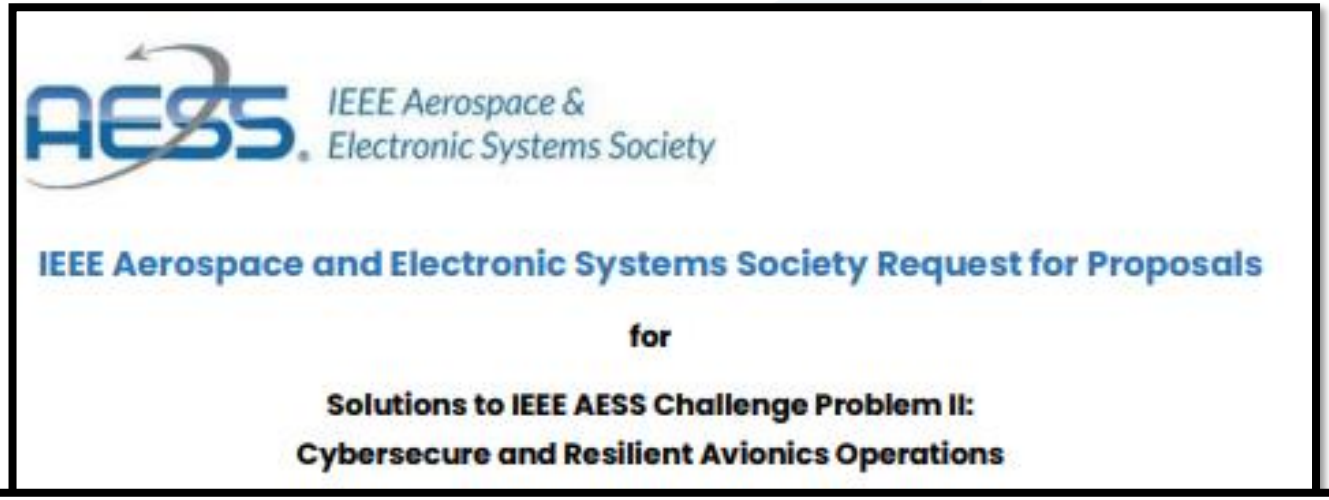
Published Software:
https://github.com/I-Fusion/drift-fairroad/tree/v2





AESS Challenge Problem

- RFP Approved by BOG and Published
- AESS Tech Panel Collaboration:
  - Avionics
  - Glue Tech for Space Systems
  - Cyber Security
- Proposals due 15 May
- Four (4) awards of $25K



IEEE Aerospace & Electronic Systems Society

IEEE Aerospace and Electronic Systems Society Request for Proposals

for

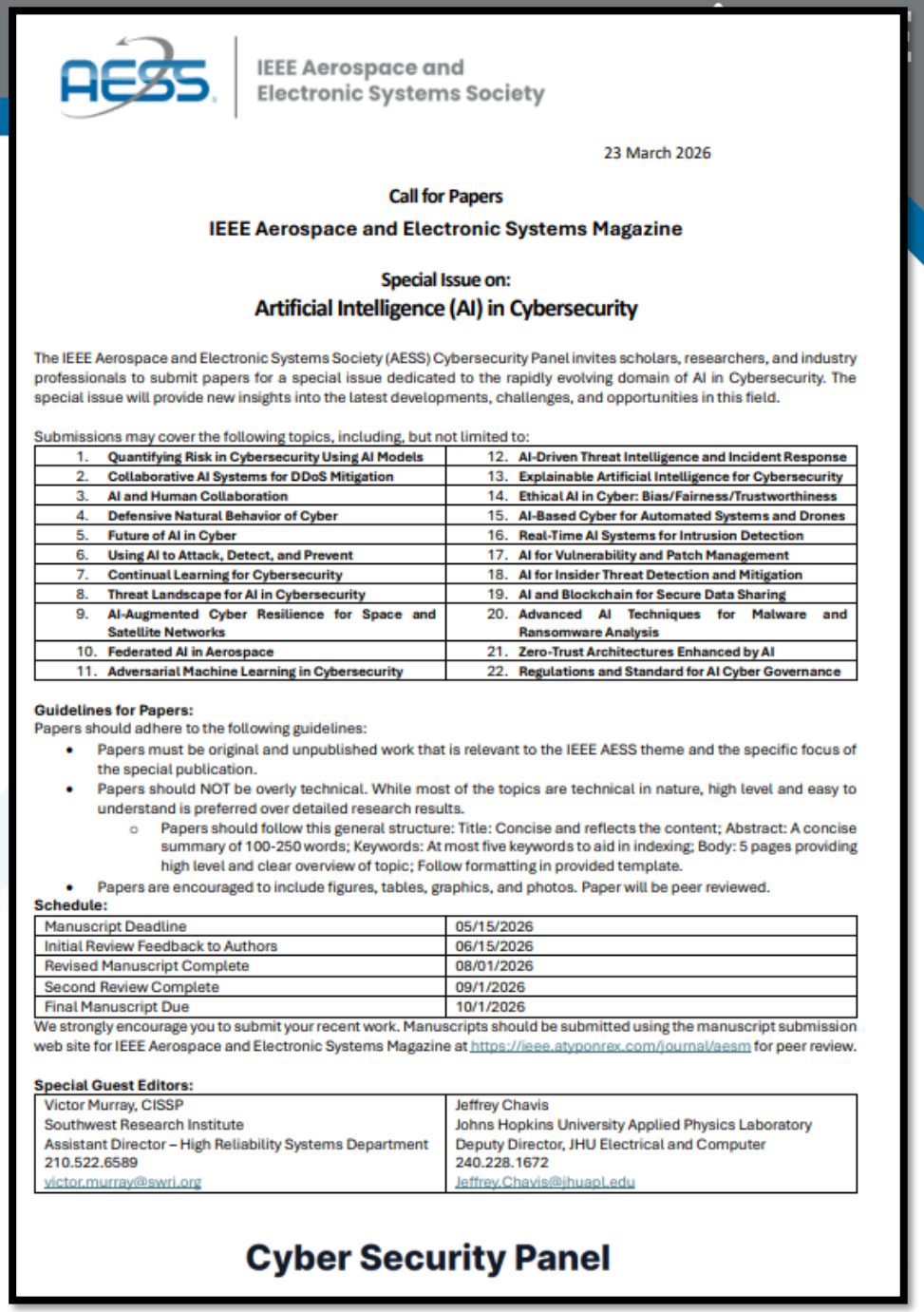
Solutions to IEEE AESS Challenge Problem II:
Cybersecure and Resilient Avionics Operations

Event	Due Date
Proposals for AESS Challenge Problem Solutions: Cybersecure and Resilient Avionics Operations	15 May 2026
Selection of four (4) Solutions for Funding	1 June 2026
Funding to Develop Solutions	15 July 2026
Technical Report and Delivery of Solutions	15 October 2026
Papers Describing Solutions for the Challenge Problem for IEEE Conference	Deadline is conference dependent.

Special Issue IEEE AESS Magazine

- Artificial Intelligence in Cybersecurity
- Jeff Chavis, Victor Murray Guest Editors
- Call for Papers Closes 13 May

Massive response from Cyber Panel Members!!!



IEEE Aerospace and Electronic Systems Society

23 March 2026

Call for Papers

IEEE Aerospace and Electronic Systems Magazine

Special Issue on:

Artificial Intelligence (AI) in Cybersecurity

The IEEE Aerospace and Electronic Systems Society (AESS) Cybersecurity Panel invites scholars, researchers, and industry professionals to submit papers for a special issue dedicated to the rapidly evolving domain of AI in Cybersecurity. The special issue will provide new insights into the latest developments, challenges, and opportunities in this field.

Submissions may cover the following topics, including, but not limited to:

1. Quantifying Risk in Cybersecurity Using AI Models	12. AI-Driven Threat Intelligence and Incident Response
2. Collaborative AI Systems for DDoS Mitigation	13. Explainable Artificial Intelligence for Cybersecurity
3. AI and Human Collaboration	14. Ethical AI in Cyber: Bias/Fairness/Trustworthiness
4. Defensive Natural Behavior of Cyber	15. AI-Based Cyber for Automated Systems and Drones
5. Future of AI in Cyber	16. Real-Time AI Systems for Intrusion Detection
6. Using AI to Attack, Detect, and Prevent	17. AI for Vulnerability and Patch Management
7. Continual Learning for Cybersecurity	18. AI for Insider Threat Detection and Mitigation
8. Threat Landscape for AI in Cybersecurity	19. AI and Blockchain for Secure Data Sharing
9. AI-Augmented Cyber Resilience for Space and Satellite Networks	20. Advanced AI Techniques for Malware and Ransomware Analysis
10. Federated AI in Aerospace	21. Zero-Trust Architectures Enhanced by AI
11. Adversarial Machine Learning in Cybersecurity	22. Regulations and Standard for AI Cyber Governance

Guidelines for Papers:

Papers should adhere to the following guidelines:

- Papers must be original and unpublished work that is relevant to the IEEE AESS theme and the specific focus of the special publication.
- Papers should NOT be overly technical. While most of the topics are technical in nature, high level and easy to understand is preferred over detailed research results.
  - Papers should follow this general structure: Title: Concise and reflects the content; Abstract: A concise summary of 100-250 words; Keywords: At most five keywords to aid in indexing; Body: 5 pages providing high level and clear overview of topic; Follow formatting in provided template.
- Papers are encouraged to include figures, tables, graphics, and photos. Paper will be peer reviewed.

Schedule:

Manuscript Deadline	05/15/2026
Initial Review Feedback to Authors	06/15/2026
Revised Manuscript Complete	08/01/2026
Second Review Complete	09/1/2026
Final Manuscript Due	10/1/2026

We strongly encourage you to submit your recent work. Manuscripts should be submitted using the manuscript submission web site for IEEE Aerospace and Electronic Systems Magazine at https://ieee.atyponrex.com/journal/aesm for peer review.

Special Guest Editors:

Victor Murray, CISSP Southwest Research Institute Assistant Director – High Reliability Systems Department 210.522.6589 victor.murray@swri.org	Jeffrey Chavis Johns Hopkins University Applied Physics Laboratory Deputy Director, JHU Electrical and Computer 240.228.1672 Jeffrey.Chavis@jhuapl.edu

Cyber Security Panel

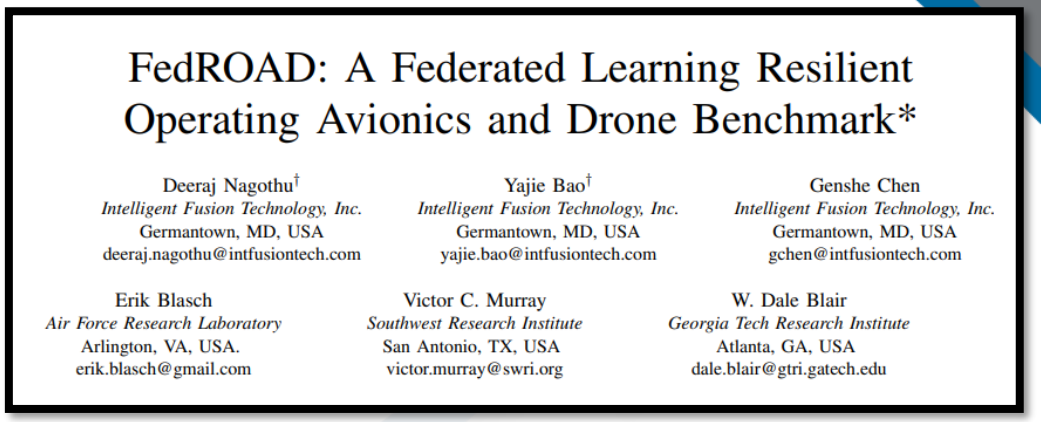
Cyber Security Panel - Spring 2025 Report

Conference Contributions

- International Carnahan Conference on Security Technology (ICCST); October 2025 Panel Discussion on AI/ML in Cybersecurity; Zechun Jacob Cao, Victor Murray, Provided Keynote Speakers
- Aerospace Cybersecurity Workshop; April 2026; Krishna Sampigethaya Keynote/Introduction, Victor Murray Panel Discussion Airport Cyber
- Flight Software Workshop - Aerospace Corporation, NASA Jet Propulsion Laboratory, and the Southwest Research Institute; March 2026; Presentation ‘Zero Trust for Avionics’; Henry Haswell
- Texas Space Cybersecurity Workshop; February 2026; Victor Murray
- Aerospace Cyber Symposium; February 2026; Krishna Sampigethaya, Victor Murray Panel Discussion; ERAU/NASA/NSF
- Airportech International Symposium; February 2026; Victor M. - Cybersecurity for Smart Infrastructure: Threats, Case Studies, and Resilience
- DASC 2025: AI in Cybersecurity Panel Discussion

Publication Activities

- FUSION 2026: Paper Accepted FedROAD: A Federated Learning Resilient Operating Avionics and Drone Benchmark
- DASC 2025: Best Cyber Paper - Model-Based Avionics Cybersecurity Framework for Identification of Risk and Evaluation
- DASC 2025: Zero Trust for Avionics
- ISSCT 2025: Technical Risk Indicators for the Critical Pathway to Insider Risk
- Risk Assessment Article Magazine Article



FedROAD: A Federated Learning Resilient Operating Avionics and Drone Benchmark*

Deeraj Nagothu†
Intelligent Fusion Technology, Inc.
Germantown, MD, USA
deeraj.nagothu@intfusiontech.com

Yajie Bao†
Intelligent Fusion Technology, Inc.
Germantown, MD, USA
yajie.bao@intfusiontech.com

Genshe Chen
Intelligent Fusion Technology, Inc.
Germantown, MD, USA
gchen@intfusiontech.com

Erik Blasch
Air Force Research Laboratory
Arlington, VA, USA.
erik.blasch@gmail.com

Victor C. Murray
Southwest Research Institute
San Antonio, TX, USA
victor.murray@swri.org

W. Dale Blair
Georgia Tech Research Institute
Atlanta, GA, USA
dale.blair@gtri.gatech.edu

Education Activities

- SPARTA – Brandon Bailey, Aerospace Corp. https://sparta.aerospace.org/
- Cyber Security Standards for Space - William Ferguson
- Transportation Cybersecurity Challenges – Edward Fok
- Insider Threat – Bill Claycomb
- Federated AI for Securing Drones – Deeraj Nagothu
- OT Cyber Analysis – Garrett Jarres
- ICCST Conference - Post Quantum Cryptography Workshop; Cameron Mott
  - Was cancelled at last minute by conference committee. Looking for opportunity to use created plans.

Industry Engagement and Standards

- P3536 - Space System Cybersecurity Design Standard Working Group
  - **Collaboration with Greg Falco, William Ferguson**
- Cleared for Contract: Navigating Compliance to Compete in Space; CyberSat; November 2025 – Greg Falco, Victor M.

Cyber Security Panel - Future Plans

- Review Challenge Problem Solution II Proposals
  - Proposal Review and Selection Committee
  - Begin Performance and Awardee Oversight
- Review Paper Submissions for IEEE AESS Special Publication: AI in Cybersecurity
- Support Conferences
- Publish Magazine Article on Risk Assessment
- Continue Cyber Panel Growth
- Continue to Host Technical Presentations
- Continue Engagement with Cyber Standards