U.S. Army Aviation Cyber Rodeo Redstone Arsenal, AL

March 31st & April 1st, 2026

AVIATION CYBER INITIATIVE

ZERO TRUST APPROACHES FOR AVIATION SYSTEMS

Rodeo Director: Veronica Bunn, FAA, veronica.v.bunn@faa.gov
Technical Director: Tom Barnett, US Army CPE Aviation, thomas.c.barnett10.civ@army.mil
Event POC: Trey Franklin, DESE Research, Inc., trey.franklin@dese.com

Event Sponsor and Coordinator DESE RESEARCH, INC.

Agenda – March 31st

Time (CT)	Topic/Presenter	Description
	Opening Session	
0800 – 0830	**Networking, Housekeeping, & Connectivity** Jasmine Savage, vFairs Support	Time will be given for attendees to arrive/connect, get settled, and for any issues to be troubleshot. Coffee and light refreshments will be provided.
0830 – 0900	**Opening Remarks** Dr. Charles L. Karr, UAH Mr. John Van Houten, US Army CPE Aviation	UAH and Army leadership will introduce the event and discuss the significance and impact of the cybersecurity work being done at both UAH and Redstone Arsenal.
0900 – 0915	**Agenda and Event Overview** Tom Barnett, US Army CPE Aviation	ACI Army leadership will provide an overview of this Army ACI Rodeo event.
0915 – 0925	**ACI Overview and Activities** Denise Hampt, DoW ACI Tri-Chair Mike Falteisek, FAA ACI Tri-Chair	ACI leadership will provide an overview of ACI and recent activities.
0925 – 0955	**Zero Trust Overview** Tom Barnett, US Army CPE Aviation	US Army ACPE(E&A) leadership will give an overview of Zero Trust and its impact to all current and future Army Aviation platforms.
0955 – 1010	**Session Break**	

Agenda – March 31st

Time (CT)	Topic/Presenter	Description
	Architectural Approaches to Zero Trust	
1010 – 1050	**Open Avionic Platform Security Architecture** Will Keegan, Lynx	Platform and data protection features in real-time systems are often intrusive and highly customized, creating significant technical and programmatic risks. Current MOSA standards focus on mission-application functional interfaces, leaving cyber integration challenges underemphasized. This presentation highlights key challenges to cyber integration on avionic systems and promotes technical benefits of platform software architecture properties and features for consideration in future industry standards and platform acquisition requirements.
1050 – 1125	**Zero Trust Threat Monitoring Technologies** Trey Franklin, DESE Research, Inc.	The Army's industry partner, DESE Research, Inc., will present and demonstrate a suite of security capabilities that can monitor, attest, and recover a compromised LRU within an aviation platform.
1125 – 1200	**Hardware Enforced Zero Trust** Reece Johnston, GDMS | Idaho Scientific	The Army's industry partner, Idaho Scientific, will explain the role of security hardware in enacting the DoW's Zero Trust guidance. As part of this, their novel secure processing technology, the Helios Processing System, will be presented. Helios is a groundbreaking secure processing technology that enforces cryptographic isolation and authentication at the cache line level—eliminating the memory corruption vulnerabilities that account for ~70% of cybersecurity attacks.
1200 – 1300	**Hosted Lunch & Virtual Exhibit Hall Hours**	

Agenda – March 31st

Time (CT)	Topic/Presenter	Description
	Device / Applications & Workloads Session	
1300 – 1305	**Session Introduction**	Session organizers will introduce the session and provide an overview of what will be shown.
1305 – 1340	**FORCE Environment** Drew Stephenson, Applied Research Solutions LaTasha Johnson, CROWS	The Army's industry partner, Applied Research Solutions, will provide an introduction to the FORCE platform and discuss how it both implements zero-trust and can support programs in zero-trust evaluation.
1340 – 1415	**Is your Aviation System as Safe as its "Memory Safe" Language?** Dr. Jonathan Hood, COLSA	Dr. Hood examines the push for "memory safe" programming languages and highlights their limitations in complex systems like aviation and missile platforms. He also offers guidance on designing custom Zero Trust Architectures (ZTAs) that incorporate memory safety measures, with enforcement policies tailored at the program level.
1415 – 1450	**Secure Compiler Extension for C/C++** Martin Cox, DESE Research, Inc.	Martin Cox is a Senior DevSecOps Scientist with a background in cyber security and security compliance. They will present how prevalent memory errors are in C/C++, how current tooling is insufficient to prevent these errors, and how SCE is currently solving these issues.
1450 – 1505	**Session Break**	

Agenda – March 31st

Time (CT)	Topic/Presenter	Description
	Device / Applications & Workloads Session (Cont'd)	
1505 – 1540	**Automated Vulnerability Prediction** Cameron White, DESE Research, Inc.	The Army's industry partner, DESE Research, Inc., will present and demonstrate Automated Vulnerability Prediction (AVP), a Machine Learning-based static analysis tool that aims to automatically detect vulnerabilities in source code. This technology massively expedites code analysis by identifying code smells, reducing manpower requirements and analysis time for large source code directories.
1540 – 1615	**Hardware Introspection Methodologies** Corwin Warner, DESE Research, Inc.	The Army's industry partner, DESE Research, Inc., will present applications, developments, and discoveries behind introspection of system memory by hardware logic, and how such an implementation differs in contrast to software/virtual memory introspection methodologies
1615 – 1650	**Zero Trust Supply Chain for Critical Electronics** Sebastian Fischmeister, Palitronica	Global chip shortages and opaque supply chains have heightened safety and security risks in electronics, as vulnerabilities can be introduced by upstream suppliers beyond immediate oversight. This presentation introduces a novel approach to cybersecurity supply chain management using RF-based characterization to implement Zero Trust principles for electronic components and assemblies to enhance the integrity of electronic systems.
1700 – 1730 (Room 114)	**Zero Trust Transceivers: Zero Trust Reference Architecture for Weapon Systems** Keith E. Miller, MITRE	MITRE's Zero Trust Transceivers (ZTX) architecture is a Zero Trust Reference Architecture designed for Operational Technology (OT) systems and in particular Weapon Systems (WS). ZTX improves mission resiliency through adoption Zero Trust principles and provides methodology for enforcing policies that balance mission, safety, and risk. This briefing will cover an overview of ZTX and a live demonstration of MITRE's latest ZTX prototype components.

Agenda – April 1st

Time (CT)	Topic/Presenter	Description
	Opening Session	
0800 – 0830	**Networking, Housekeeping, & Connectivity** Jasmine Savage, vFairs Support	Time will be given for attendees to arrive/connect, get settled, and for any issues to be troubleshot. Coffee and light refreshments will be provided.
0830 – 0840	**Session Introduction** Tom Barnett, US Army CPE Aviation	Session organizers will introduce the session and provide an overview of what will be shown.
0840 – 0915	**MITRE Resilient Cyber Aerospace Testbed Capabilities Overview** Keith E. Miller, MITRE	MITRE's Resilient Cyber Aerospace Testbed (RCAT) Lab provides a collaborative cyber/avionics testbed for platform research shared across government agencies, industry, and academia. Hosting several capabilities including configurable cockpit simulators, subsystem test-benches, and a light sport commercial aircraft for testing, the RCAT lab provides an environment for developing and testing mission resilience capabilities.
0915 – 0950	**TAPO/SIMO Cybersecurity Posture & Strategic Roadmap** Chris Abbott (TAPO) Alan Fiorello (TAPO) Joe Morra (SIMO) Luke Carpenter (NIWC)	This session provides an update on TAPO/SIMO's cybersecurity efforts, including recent accomplishments and a strategic path forward. We'll discuss challenges, proposed solutions, and opportunities for program office collaboration in order to protect critical warfighter capabilities.

Agenda – April 1st

Time (CT)	Topic/Presenter	Description
	Applications & Workloads / SBOM Session	
0950 – 1005	**Session Break**	
1005 – 1040	**SBOM Generation and Attack Surface Reduction** Erik MacIntyre, DESE Research, Inc.	The Army's industry partner, DESE Research, Inc., will present and demonstrate SBOM Generation and Attack Surface Reduction utilizing the Embedded Attack Surface Reduction (EASR) GOTS tool. EASR provides the capability to analyze and automatically remove file- and function-level dependencies in an embedded system and can generate an enriched SBOM with the analysis data.
1040 – 1115	**Software Supply Chain Illumination Platform (SSCIP)** Bill Baker, DESE Research, Inc.	The Army's industry partner, DESE Research, Inc., will present and demonstrate the Software Supply Chain Illumination Framework (SSCIP). This Army owned application manages a collection of Software Bill of Materials (SBOMs) by providing vulnerability notification and asset management as well as contributor details for open-source dependencies.
1115 – 1150	**High Assurance Containerization Architecture** Michael Doran, DornerWorks	The Army's industry partner, DornerWorks, will present and demonstrate High-Assurance Container Architecture (HACA), a secure architecture built on the formally verified seL4 microkernel and designed to provide strong isolation for containerized workloads and orchestration.
1150 – 1300	**Hosted Lunch & Virtual Exhibit Hall Hours**	

Agenda – April 1st

Time (CT)	Topic/Presenter	Description
	Academia and Industry Session	
1300 – 1305	**Session Introduction**	Session organizers will introduce the session and provide an overview of what will be shown.
1305 – 1340	**AeroSync Quantum Resiliency** Noel Grover, EnQuanta	The Army's industry partner, EnQuanta, will present and demonstrate a quantum-resilient cryptography upgrade to the Astronautics AeroSync platform.
1340 – 1415	**Astronautics Cyber Methodology and Tools** Kathleen Finke, Astronautics	The Army's industry partner, Astronautics, will present and demonstrate some of the cybersecurity analysis tools and processes designed to support embedded systems, such as weapon systems and aircraft. Developed to support the certification and continued airworthiness processes of DO-326 and DO-356. Starting with modeling and simulation of risk during the design phase, to support early inclusion of mitigation strategies, to the identification and classification of vulnerabilities found in commercial off-the-shelf (COTS) software and firmware utilizing bills of materials (BOMs).
1415 – 1450	**Know Your Network: The Vibrant System** Tim Kesecker, Securboration	The Army's industry partner, Securboration, will present and demonstrate the Vibrant system. The Vibrant system consists of a flight certified Mil-Spec hardware component that connects to the aircraft on-board data buses (Mil-Std-1553, ARINC-429). All bus data is captured, recorded, and decoded per defined ICDs, for real-time or post-mission analysis. The Vibrant System provides user-defined device health and performance metrics as well as custom visualization and analytics for each platform.

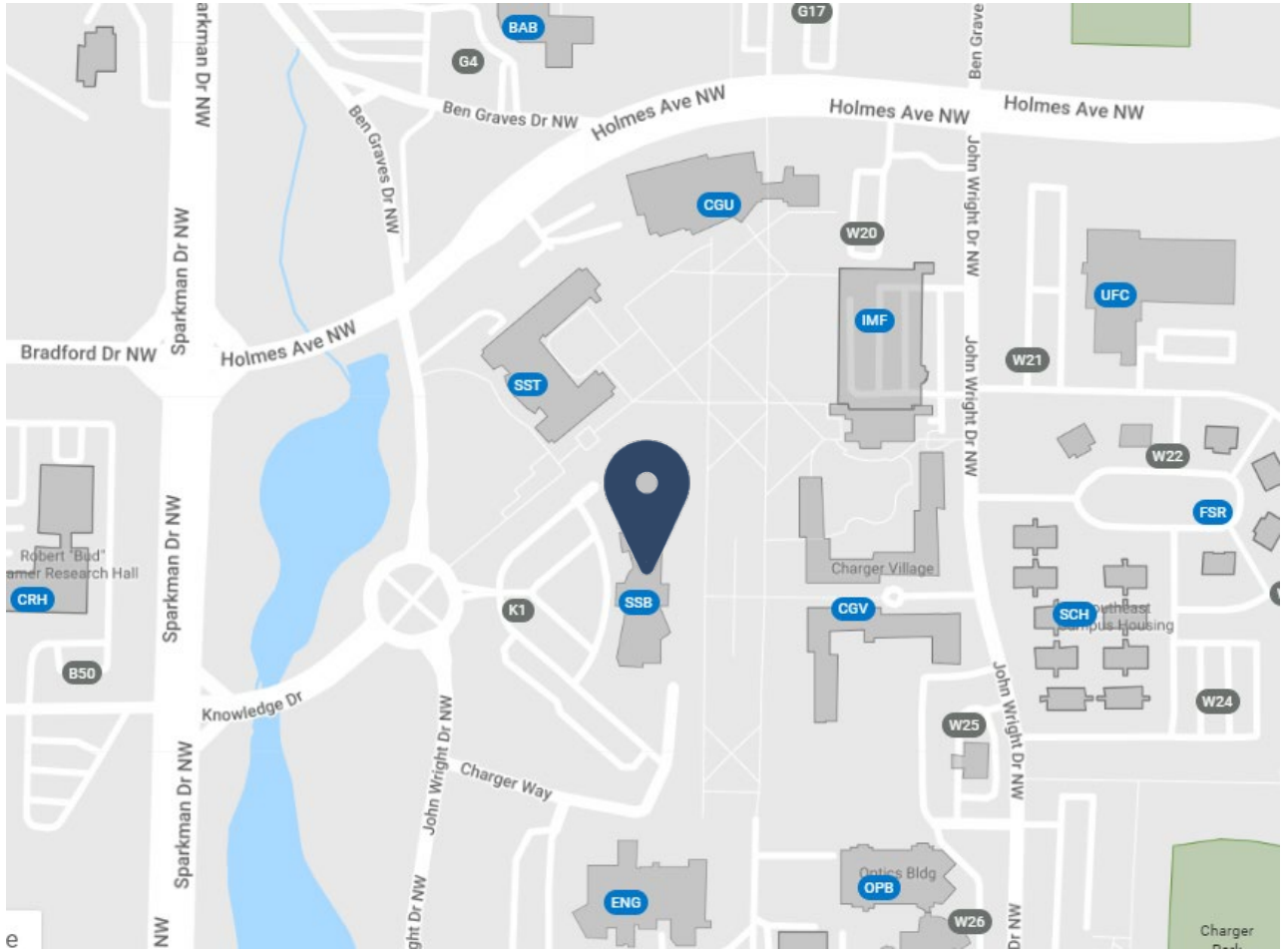
Agenda – April 1st

Time (CT)	Topic/Presenter	Description
Academia and Industry Session (Cont'd)		
1450 – 1500	**Session Break**	
1500 – 1535	**Why Traditional Defenses are Not Enough: Exploring Recent, Cutting-Edge Attack Techniques** Dr. Bramwell Brizendine, UAH	The University of Alabama in Huntsville will discuss two recent attack techniques, process injection via Return-Oriented Programming (ROP) and automated, universal ASLR bypasses – demonstrating why some common controls (EDR, DEP, ASLR) are insufficient on their own, as attackers often find ways to bypass existing mitigations.
1535 – 1610	**First Principles Approach to TRNG Circuits** Micah Tseng, UAH	The University of Alabama in Huntsville will present approaches for entropy generation that are grounded in first principles theory. UAH will also present circuits and theory that support a straightforward understanding of information generated as opposed to a posteri statistical testing.
1610 – 1645	**Zero Trust in the Skies: Lessons from Aviation Architectures for DoD Networks** Sean Crouse, Ph.D., ERAU Dan Diessner, ERAU (Co-Author)	Zero Trust Architecture (ZTA) has become a cornerstone of the Department of Defense's cybersecurity modernization strategy, with the Networks pillar serving as its foundation. This presentation explores how aviation architectures reflect many ZTA principles. By examining how aircraft networks are structured, why safety system architectures are so resilient, and how flight-critical systems enforce segmentation and redundancy, we reveal striking parallels to Zero Trust concepts such as microsegmentation, least privilege, continuous monitoring, and "assume breach" design. The session will also map aviation lessons across multiple ZTA pillars, providing practical insights for strengthening DoD networks and mission systems

Location

UAH Student Services Building (SSB)

- Auditorium/Room 112
- 301 Sparkman Dr NW, Huntsville, AL 35899
- 34.72470, -86.64061
- POC: Sharon Johnson, 256-457-8483



Accommodations and Airports

Accommodations

- **Huntsville Marriott at the Space & Rocket Center**
  - 5 Tranquility Base, Huntsville, AL 35805
  - 256-830-2222
  - 1.4 miles [4-Minute drive]
- **Hilton Garden Inn Huntsville/Space Center**
  - 4801 Governors House Dr SW, Huntsville, AL 35805
  - 256-430-1778
  - 1.3 miles [4-Minute Drive]
- **106 Jefferson Huntsville, Curio Collection by Hilton**
  - 106 Jefferson St S, Huntsville, AL 35801
  - 256-288-0128
  - 5 miles [8-Minute Drive]
- **The Westin Huntsville**
  - 6800 Governors W, Huntsville, AL 35806
  - 256-428-2000
  - 3.3 miles [9-minute Drive]
- **Four Points by Sheraton Huntsville Airport**
  - 1000 Glenn Hearn Boulevard, Huntsville, AL 35824
  - 256-772-9661
  - 9.7 miles [18-Minute drive]

Airport(s)

- **Local:**
  - Huntsville International Airport (HSV)
- **Driving Distance:**
  - Birmingham-Shuttlesworth International Airport (BHM) [1.5-Hour Drive]
  - Nashville International Airport (BNA) [2-Hour Drive]

Dining

Nearby

- **Governor's Drive:**
  - Taqueria El Cazador, Stovehouse (256-678-7047)
  - Straight to Ale, Campus 805 (256-801-9650)
  - Gold Sprint Coffee
- **Midcity Area:**
  - Viet Huong (256-890-0104)
  - Kamado Ramen (256-964-6826)
  - Tous Les Jours (256-270-7168)
  - Salt Factory Pub (256-585-2488)
  - Rosie's Mexican Cantina (256-922-1001)
  - Chipotle (256-895-7761)
- **Bridge Street Town Center:**
  - Connors Steak & Seafood (256-327-8425)
  - Agave & Rye Epic Tacos (256-203-5788)
  - Panera Bread (256-971-1235)

Area

- **Downtown Area:**
  - Purveyor (256-419-2555)
  - The Poppy and Parliament (256-715-7152)
  - L'Etoile Patisserie (256-460-6309)
  - Canadian Bakin (256-489-2323)
  - Jack Brown's Beer & Burger Joint (256-270-7045)
- **Town Madison:**
  - J. Alexander's Restaurant (256-870-7100)
  - Prohibition Rooftop Bar & Grill (256-325-4438)
  - Super Chix (256-325-4063)
- **Redstone Gateway:**
  - Rocket City Tavern (256-319-3333)
  - Fiero Mexican Grill (256-319-3310)

Huntsville Area Information

WELCOME TO THE HUNTSVILLE/MADISON COUNTY COMMUNITY! Huntsville is a great place to live, work, and play. Decades ago, Huntsville played a major role in sending man to the Moon. Now, the Rocket City is powering NASA's Space Launch System, which will take us back to the Moon, then on to Mars! We continue with advancements in military and space – we are home to Redstone Arsenal, a Federal Center of Excellence with more than 75 federal organizations and commands including NASA's Marshall Space Flight Center, the four-star U.S. Army Materiel Command, and an FBI presence that is growing by the day (and soon, SPACE COMMAND!). Huntsville is also home to one of Alabama's top tourist destinations, the U.S. Space & Rocket Center. Huntsville and Madison County offer a high quality of life. In 2022, U.S. News & World Report named our city the No. 1 Best Place to Live in the country! We have consistently ranked in the magazine's top cities the past several years, including for affordability.

Check out Huntsville's Destination Guide below:

2025 Huntsville Destination Guide