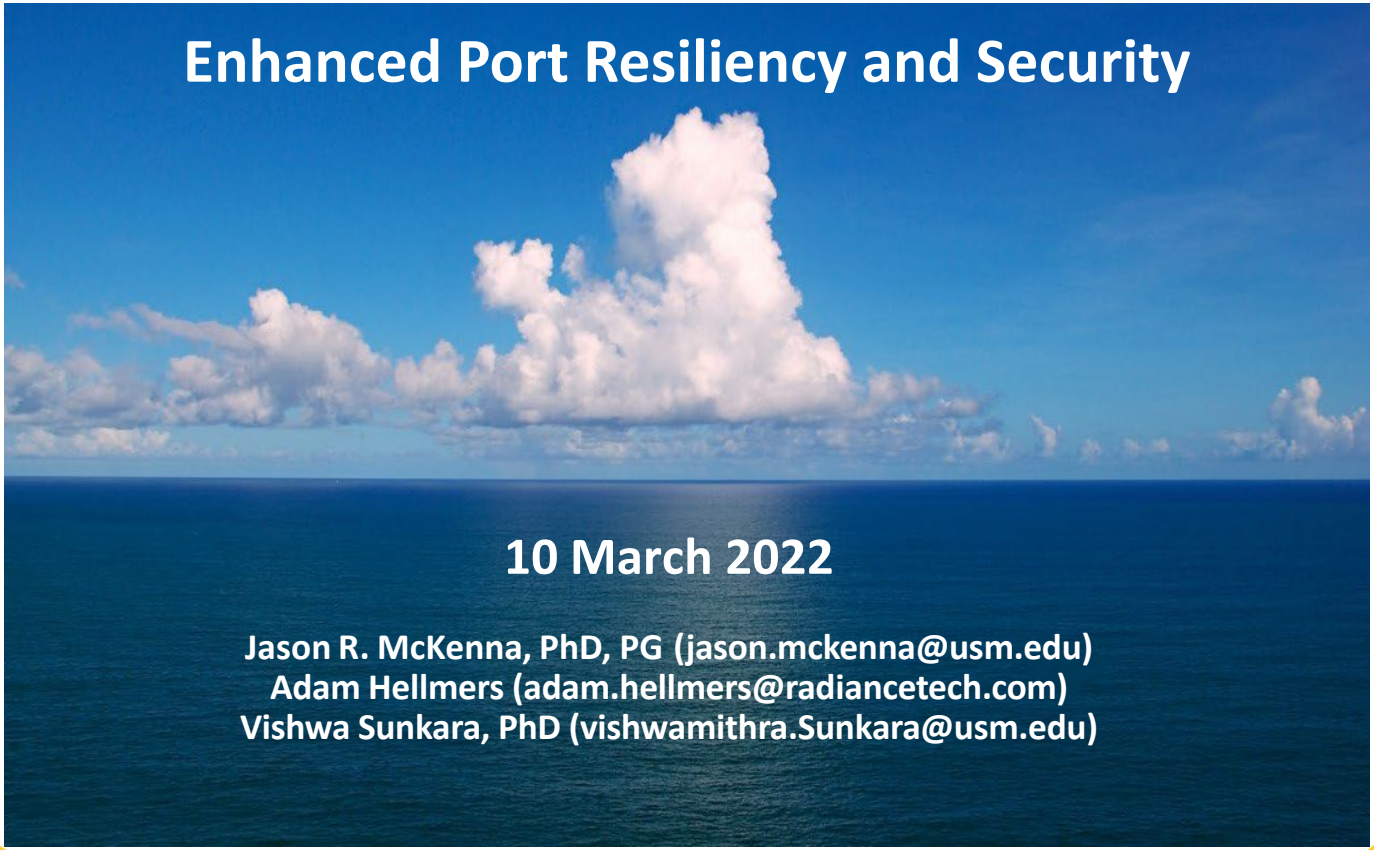
THE UNIVERSITY OF SOUTHERN MISSISSIPPI

Enhanced Port Resiliency and Security



10 March 2022

Jason R. McKenna, PhD, PG (jason.mckenna@usm.edu)
Adam Hellmers (adam.hellmers@radiancetech.com)
Vishwa Sunkara, PhD (vishwamithra.Sunkara@usm.edu)

RADIANCE TECHNOLOGIES

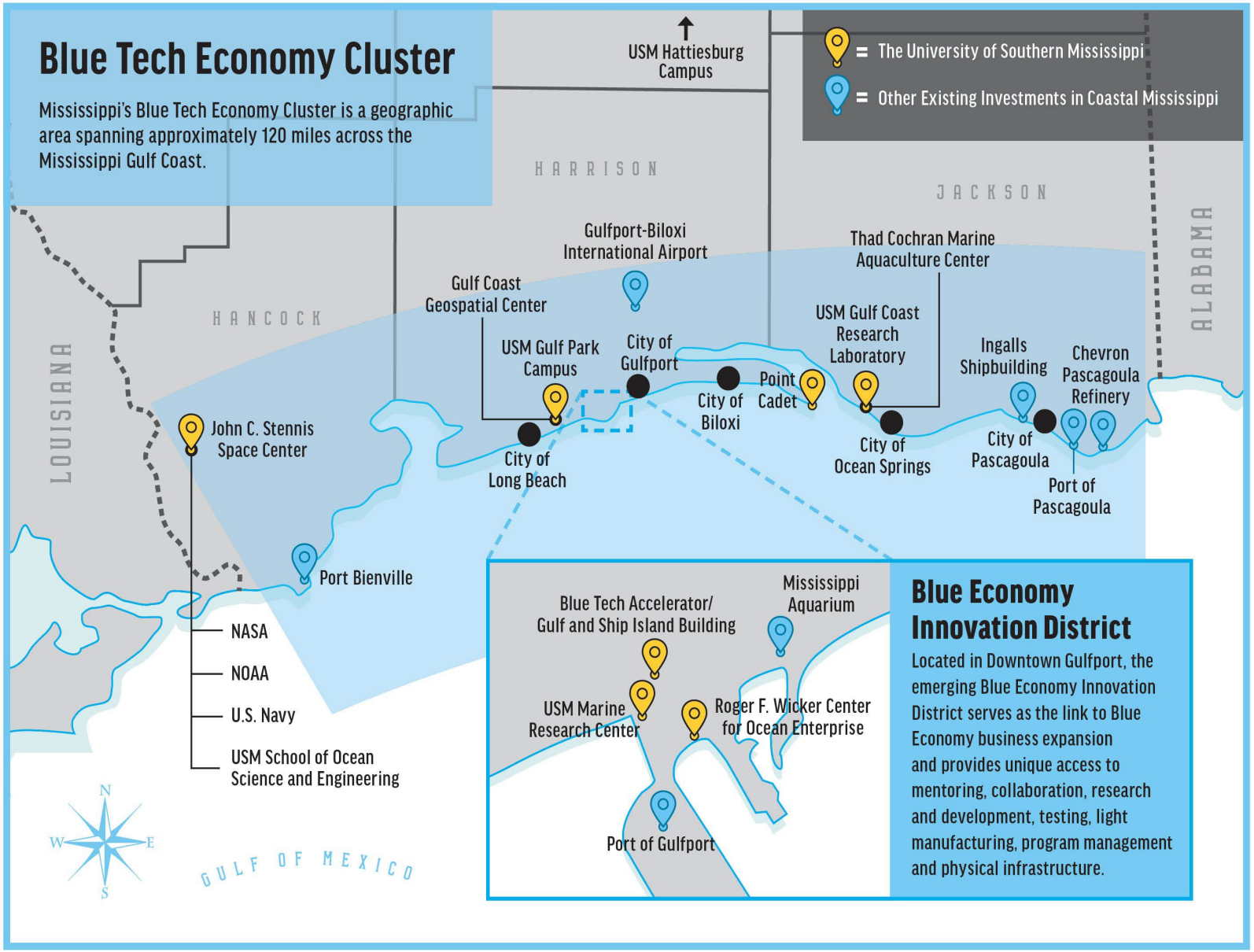
Outline

- Who we are
- Notational HITL Testbed
- RF Mapping
- AI/ML Approaches
- Way Ahead

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

RADIANCE TECHNOLOGIES

Roger F. Wicker Center for Ocean Enterprise: MRC, GSI & OEF (Port of Gulfport, Gulfport, MS)


Blue Tech Economy Cluster
Mississippi's Blue Tech Economy Cluster is a geographic area spanning approximately 120 miles across the Mississippi Gulf Coast.
USM Hattiesburg Campus
= The University of Southern Mississippi
= Other Existing Investments in Coastal Mississippi
HARRISON
JACKSON
HANCOCK
LOUISIANA
ALABAMA
Gulfport-Biloxi International Airport
Gulf Coast Geospatial Center
Thad Cochran Marine Aquaculture Center
USM Gulf Park Campus
City of Gulfport
USM Gulf Coast Research Laboratory
Ingalls Shipbuilding
Chevron Pascagoula Refinery
Point Cadet
City of Biloxi
John C. Stennis Space Center
City of Long Beach
City of Ocean Springs
City of Pascagoula
Port of Pascagoula
Port Bienville
NASA
NOAA
U.S. Navy
USM School of Ocean Science and Engineering
N
W
E
S
GULF OF MEXICO
Blue Tech Accelerator/ Gulf and Ship Island Building
Mississippi Aquarium
USM Marine Research Center
Roger F. Wicker Center for Ocean Enterprise
Port of Gulfport
Blue Economy Innovation District
Located in Downtown Gulfport, the emerging Blue Economy Innovation District serves as the link to Blue Economy business expansion and provides unique access to mentoring, collaboration, research and development, testing, light manufacturing, program management and physical infrastructure.

7.24.20

WHO WE ARE

RADIANCE TECHNOLOGIES

We are an employee-owned R&D company performing technical intelligence, developing advanced technologies, and providing engineering services.

$335M Revenue

Our focus in on providing technology solutions for the DOD and Intelligence Community.

950+ Employee-Owners

We are 100% employee owned, meaning that every employee at Radiance has a stake in the company.

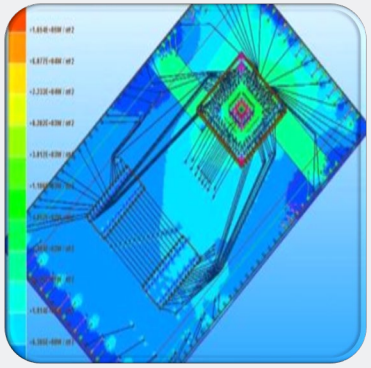
24 IDIQ/BPA Prime Contracts

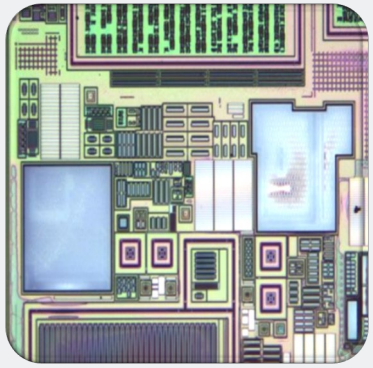
We have the established processes, tools, and expertise to prime 90% of our work.

9 Corporate Locations

We go where we are needed the most. Radiance has 11 offices and 22 project offices in 17 states coast to coast.

Capabilities



High Powered RF, HPM, E&M

- HPM Effects and VA
- HPM Failure Analysis
- HPM Source Development
- HPM C-UAV Support and Teaming
- Microelectronics HPM Effects Studies

Microelectronics Technology

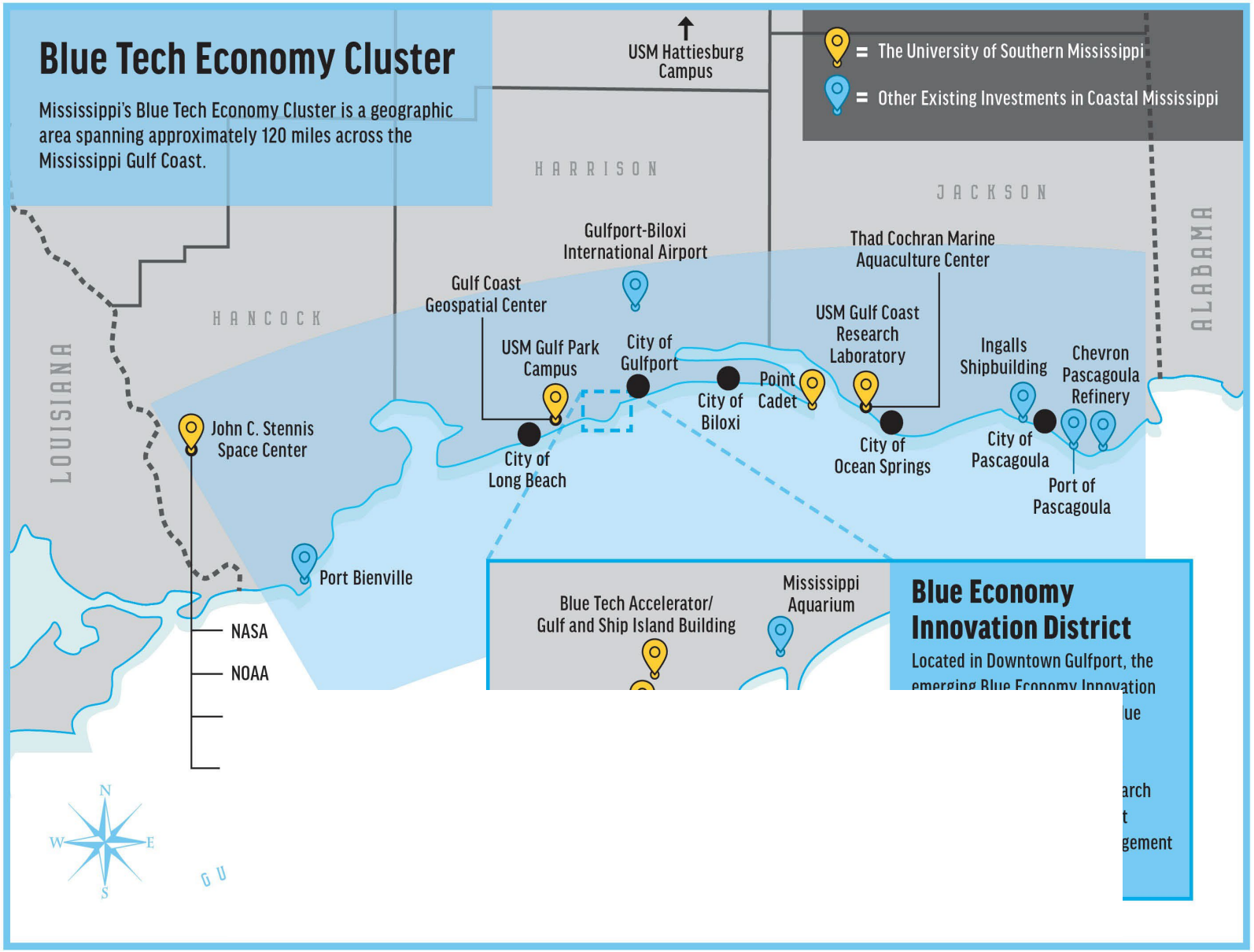
- Anti-Tamper and Embedded Cyber Defense Solutions
- Integrated Circuit Failure Analysis
- Microelectronics Exploitation
- Secure ASICs and Component Protection
- Solutions to protect Technology vital to National Security

Cyber Technologies

- Cyber Vulnerability Assessments
- Critical Infrastructure Cyber-Physical Security
- Cyber Security of AF Weapon Platforms
- Embedded System Vulnerability Analysis

Advanced Technology Development

- Secure Computer Intelligence
- Fundamental A.I./M.L. Research
- Trustworthy Code and Secure Processor Research
- IoT Security and Exploitation R&D
- Commercial AT Products and Solutions


Blue Tech Economy Cluster
Mississippi's Blue Tech Economy Cluster is a geographic area spanning approximately 120 miles across the Mississippi Gulf Coast.
USM Hattiesburg Campus
= The University of Southern Mississippi
= Other Existing Investments in Coastal Mississippi
HARRISON
JACKSON
ALABAMA
HANCOCK
LOUISIANA
Gulfport-Biloxi International Airport
Thad Cochran Marine Aquaculture Center
Gulf Coast Geospatial Center
USM Gulf Park Campus
City of Gulfport
USM Gulf Coast Research Laboratory
Ingalls Shipbuilding
Chevron Pascagoula Refinery
City of Biloxi
Point Cadet
John C. Stennis Space Center
City of Long Beach
City of Ocean Springs
City of Pascagoula
Port of Pascagoula
Port Bienville
Blue Tech Accelerator/ Gulf and Ship Island Building
Mississippi Aquarium
Blue Economy Innovation District
Located in Downtown Gulfport, the
NASA
NOAA
N
W
E
S
7.24.20

Improving Port Resiliency by Implementing a Hardware-in-the-Loop Testbed

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

RADIANCE TECHNOLOGIES

- Dynamic Testbed to test new security configurations before going live
- Sandboxed environment to validate vulnerabilities in software such as Navis' N4 Terminal Operating System
- Real-Time Multi-Domain Simulation to model full spectrum port operations
- Integrated field used hardware for ensured attack surface and event responses
- Customizable event scenarios for validation and training
- Identification of risk and testing of countermeasures in a sandboxed environment to ensure no impact to services
- Scalable scenarios for long term support and growth
- Modular capability able to support a broad range of Port Locations

Background 1

- Within any multi-domain operation (MDO) such as a Port there exists complex interconnected relationships across the land/sea/air/cyber domains.
- For example, a Crane can be loading/unloading cargo, vessels can be navigating the harbor and adjacent channels, communications can be occurring between the operations center, ocean vessels, unmanned systems, personnel, and SCADA systems or electronic smart grids can be interacting to power the communica

Background 2

- All these different operations (or systems) have some level of cross dependency. Performing security both in the digital and physical space in these complex environments, however, is challenging. For example, testing new capabilities, software, and procedures in live systems often poses significant logistic challenges and risk to the mission. Consequently, the development of cyber simulations to secure facilities with these System-of-Systems or Multi-Domain Operations locations (such as ports) is more feasible using test platform for initial validation of both the present security posture and the development of future enhancements. However, it is often impossible to fully simulate each components function and attack surface in its entirety and have a simulation run at full scale.
- Hardware-in-the-Loop (HIL) solutions for simulation events offers a hybrid approach capable of simulating the full systems function, and then selecting specific domains for various scenarios. As a result, the simulation can dynamically select a higher fidelity component for iteratively fine-tuning simulations. This allows for a higher fidelity simulation for the specific targets of interest in each scenario.

Background 3

- Finally, integrating actual hardware/software found within Port operations to interact with the simulation in real time ensures that the security of that selected hardware directly mirrors the actual physical space
- A tiered approach allows the Testbed to use abstracted models, digital twins, and physical hardware in an optimal format such that the full system can interact in real time with the hardware and the users can see the full reaction of the system to events.
- Our team's approach to HIL testbed development for MDO environments consists of the following

- Baseline of Security Posture for Typical Operations (Cargo/Vessel/Interagency Comms) using Navis' N4 Terminal Operating Systems (for example) or other nationally used TOS or Cargo Tracking software*
- Testbed Architecture Development*
- Scenario Hardware Selection and Integration*
- Scenario Development & Extensible MDO Simulation Creation **
- Component Digital Twin Development**
- Security Penetration Scenario Development**
- System Refinement***
- Training***

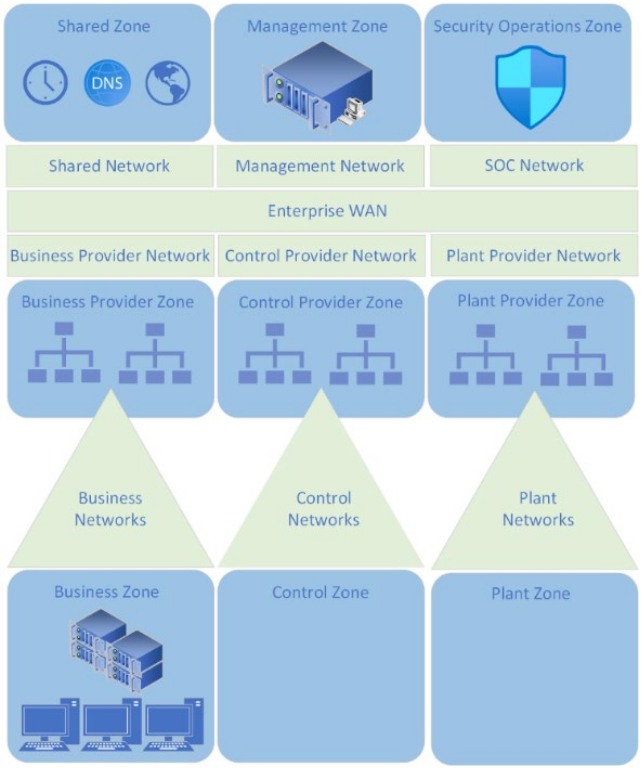
Outcome: A scalable security research testbed to support the design and development of tactics, techniques, and procedures for effective threat response to critical maritime infrastructure.

Cyber Modeling Approach

Modeling ICS components with various degrees of fidelity depending on simulation requirements

Outcome: A scalable security research testbed to support the design and development of tactics, techniques, and procedures for effective threat response to critical maritime infrastructure.

Cyber Modeling Example



Example Deployed Adaptable Testbed Architecture

Outcome: A scalable security research testbed to support the design and development of tactics, techniques, and procedures for effective threat response to critical maritime infrastructure.

Testbed Architecture

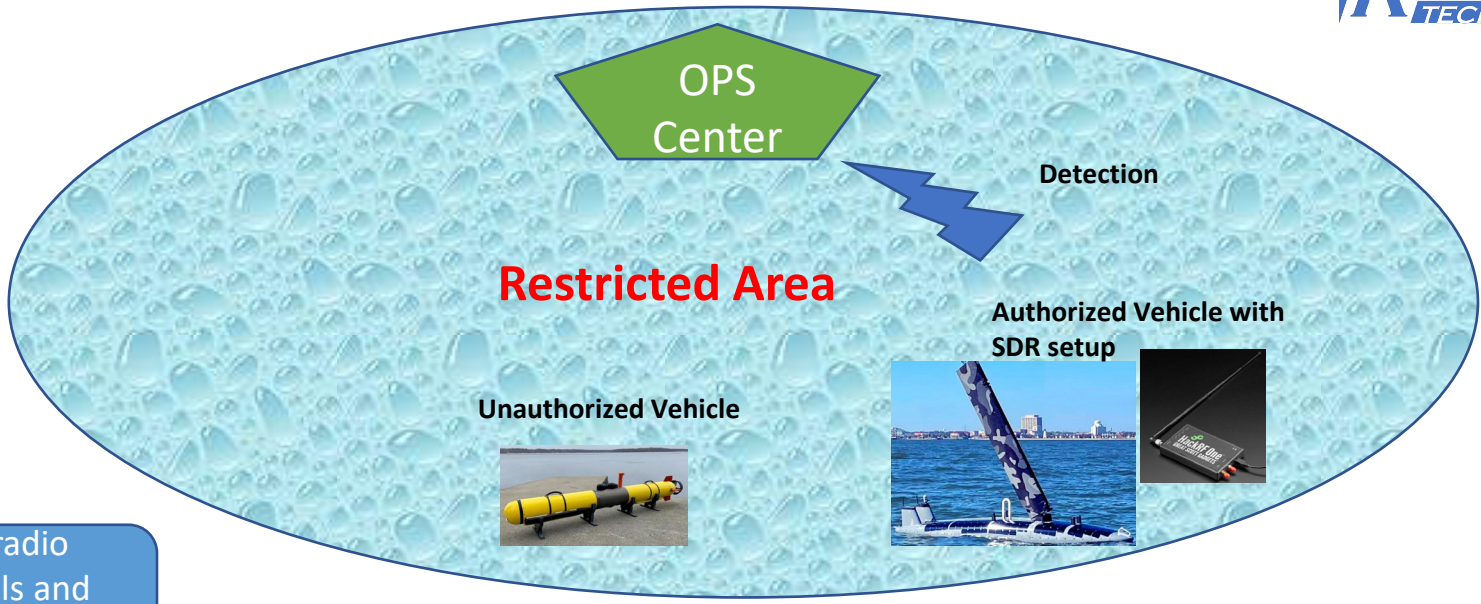
- Fully adaptable Architecture capable of deploying a PERA architecture or other 5-7 level network architecture
- Virtualizes down to the component level (Level 1) with a simulated Level 0 process dependent on the selected scenario
- Using HIL for selected level 1 component allows for attack surfaces identical to those in the field
- The adaptable testbed architecture ensures that the testbed can meet and replicate the architecture of the smallest to largest port
- **Status: Notional design complete**
- **Status: Still in requirements gathering phase**

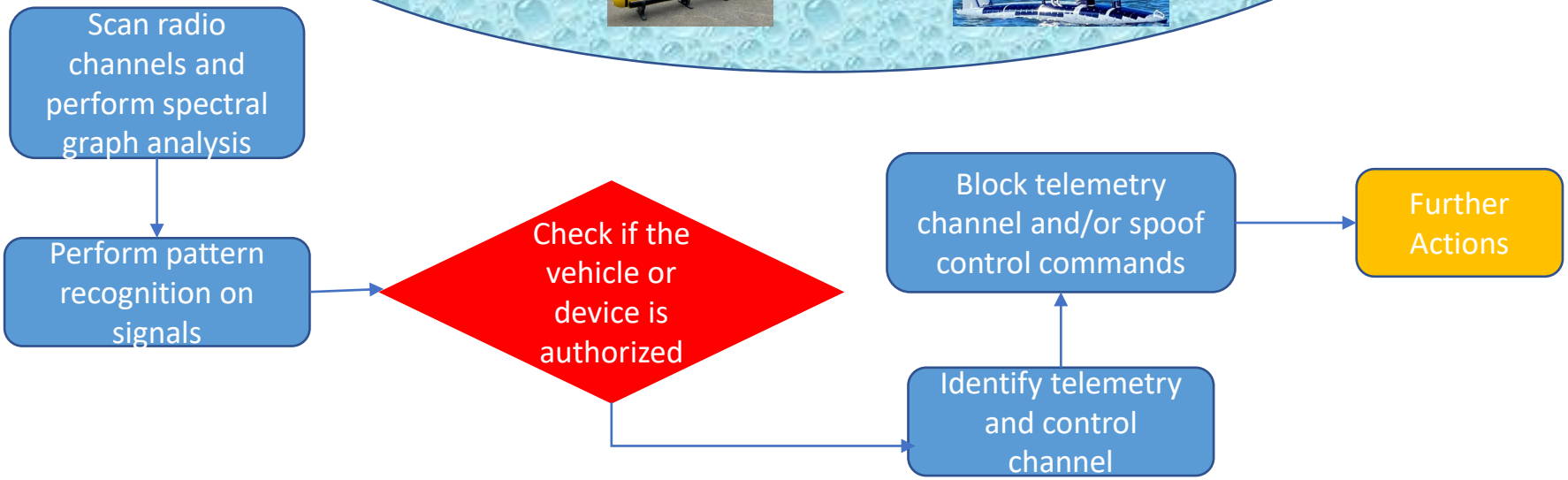
Outcome: A scalable security research testbed to support the design and development of tactics, techniques, and procedures for effective threat response to critical maritime infrastructure.

Using Software Defined Radios (SDR) for Improving Port Resiliency

- Uncrewed maritime vehicles (and UAS) have become widely available, and their potential unlawful usage and presence in restricted areas introduces new security risks.
  - It is highly desirable to restrict the unauthorized usage of uncrewed maritime vehicles and in fact any unauthorized vehicle in certain areas like ports, airports, military areas, etc.
- Unmanned vehicles are remotely controlled using radio signals and communicate with other devices and vehicles using radio signals.
- An SDR is a radio communication system that contains various reconfigurable software-based components for processing and converting digital signals.
  - Unlike traditional radio communication systems, these radio devices are highly flexible, versatile, configurable, and less expensive.
- SDRs can be used to listen to specific radio frequencies, jam GPS signals, detect use of unauthorized radio frequencies, classify and cluster authorized radio frequencies, etc.

Using Software Defined Radios (SDR) for Improving Port Resiliency : CONOP

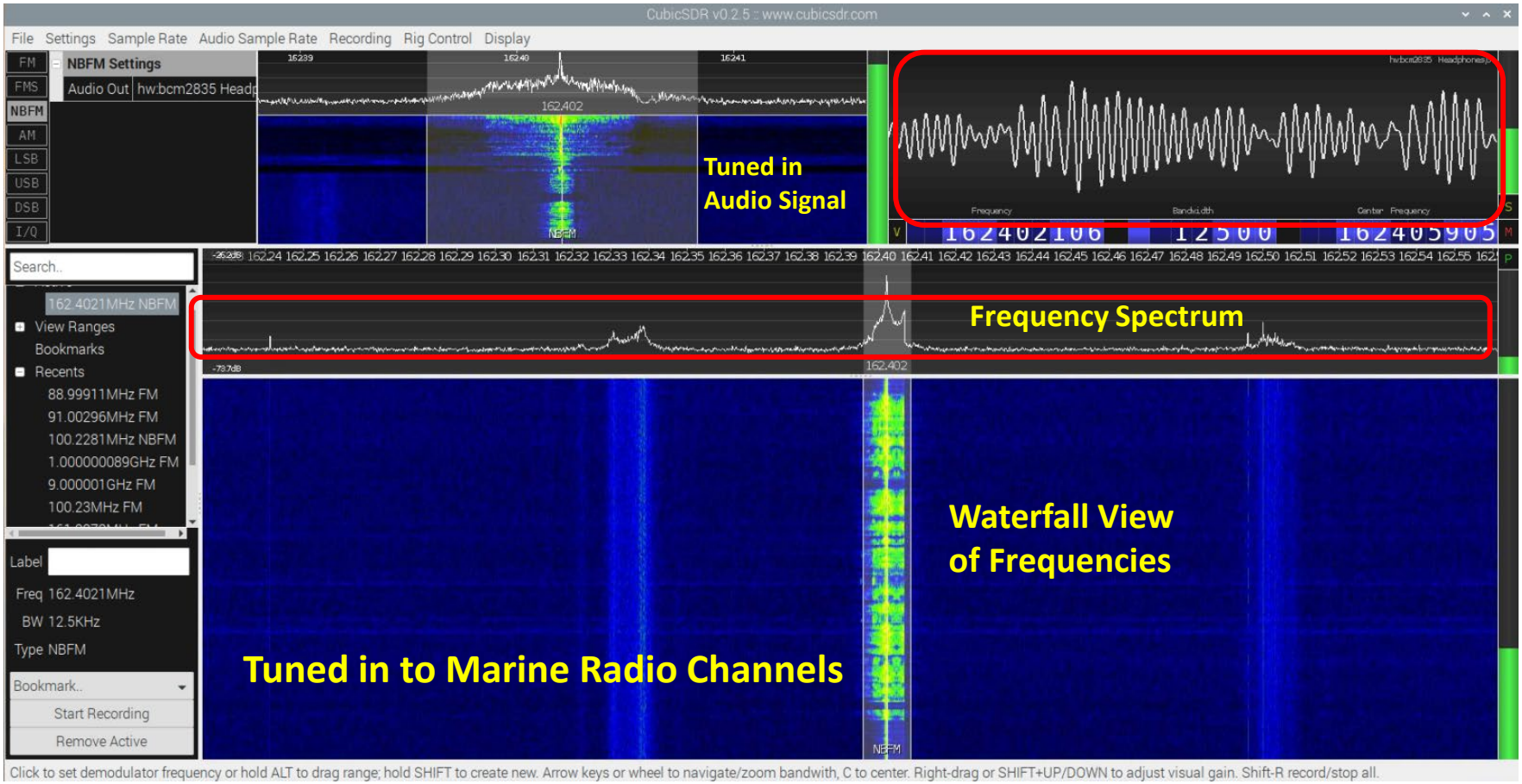




Using Software Defined Radios (SDR) for Improving Port Resiliency

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

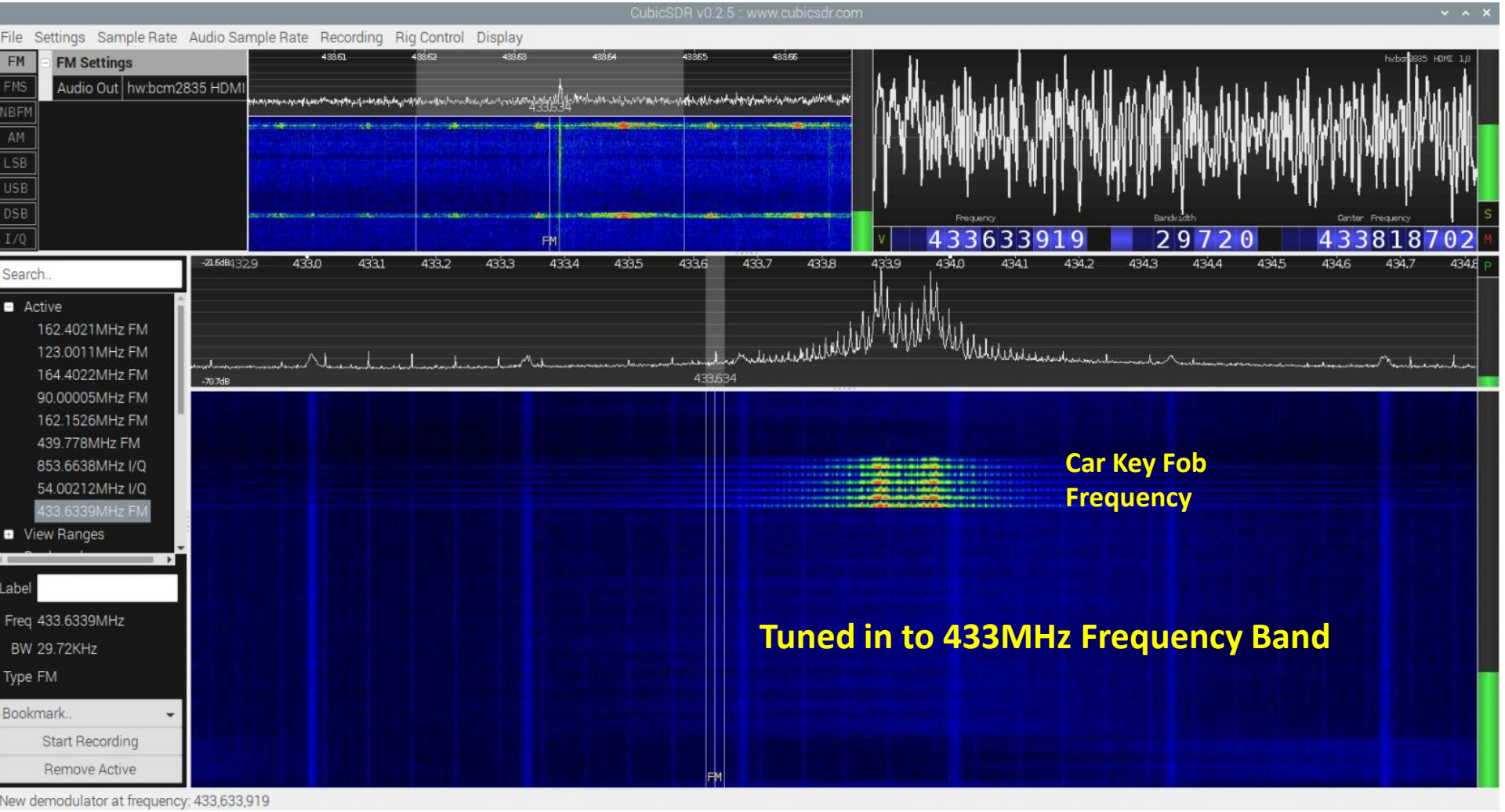
RADIANCE TECHNOLOGIES



Using Software Defined Radios (SDR) for Improving Port Resiliency

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

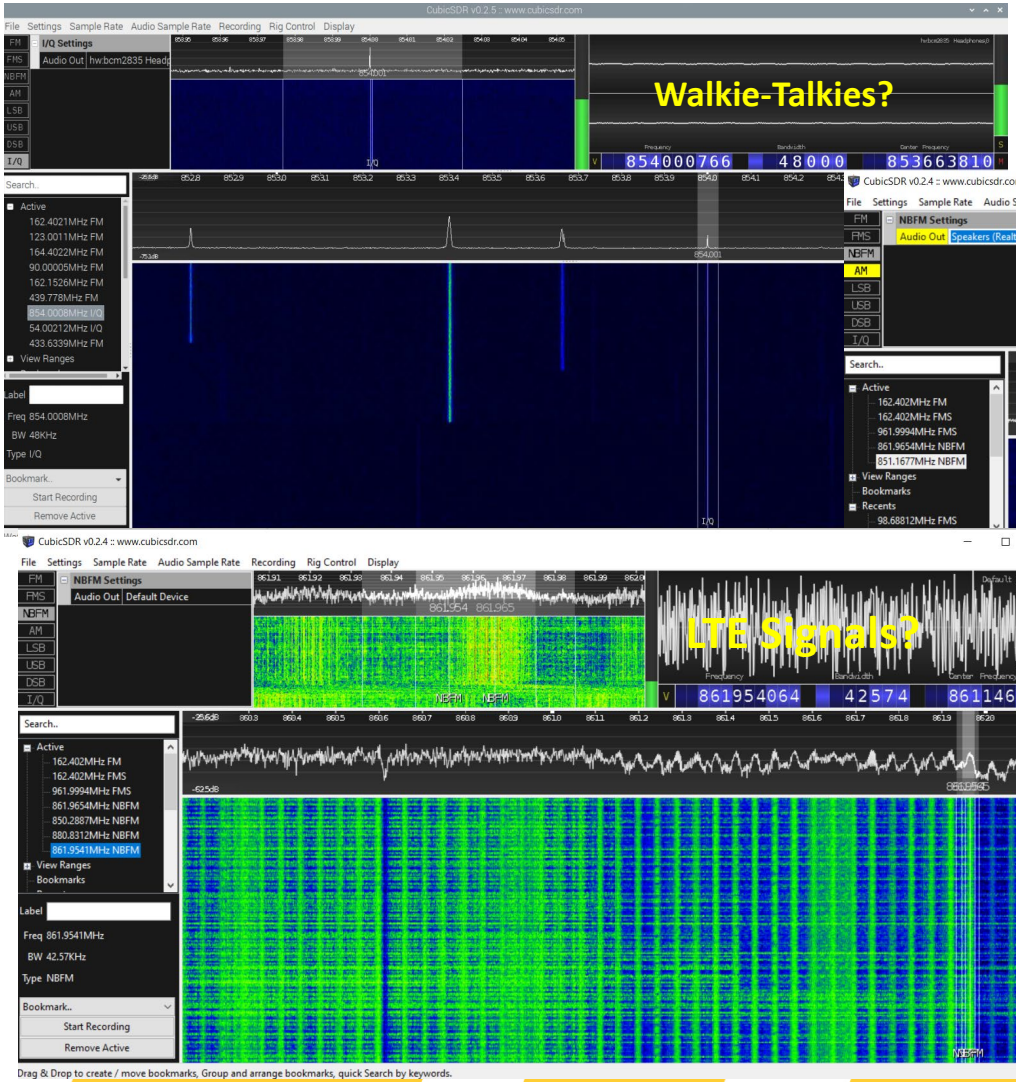
RADIANCE TECHNOLOGIES



Using Software Defined Radios (SDR) for Improving Port Resiliency

THE UNIVERSITY OF SOUTHERN MISSISSIPPI

RADIANCE TECHNOLOGIES



Summary

- Port Resiliency can be improved by implementing a Hardware-in-the-Loop Testbed
  - Can support enhanced Physical Security as well as cyber security
- RF equipped UxS can also support Port Resiliency
- Future efforts will automate data analysis and reporting