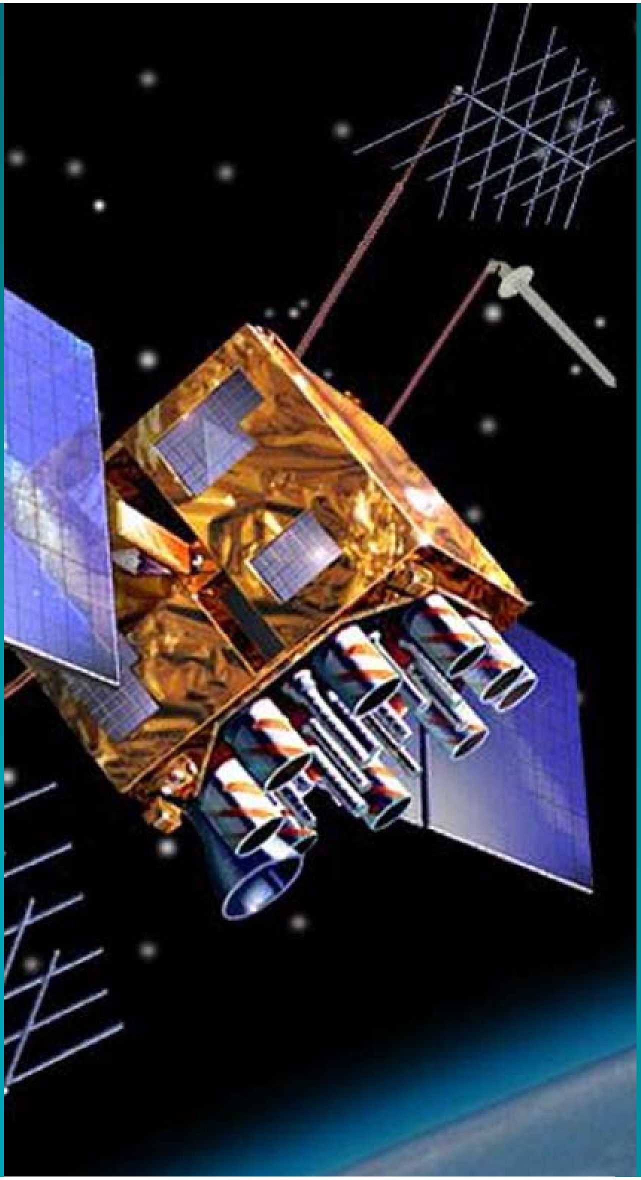
Booz | Allen | Hamilton®



SATSIM

A GPS Simulator for Cyber Testing & Exploration

DECEMBER 2022

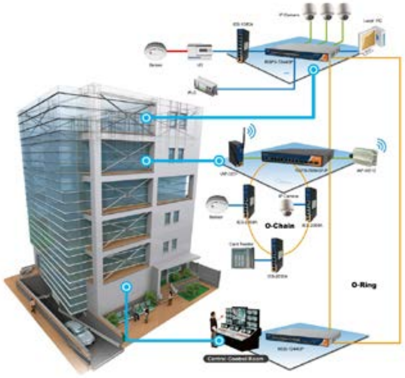
CYBER-PHYSICAL AREAS OF INTEREST

Booz Allen Hamilton is engaging with partners to develop unique test platforms where complex systems require specialized knowledge and tools, ranging from pure software simulations to fully-realized hardware SILs.

Satellites & Space

Aviation

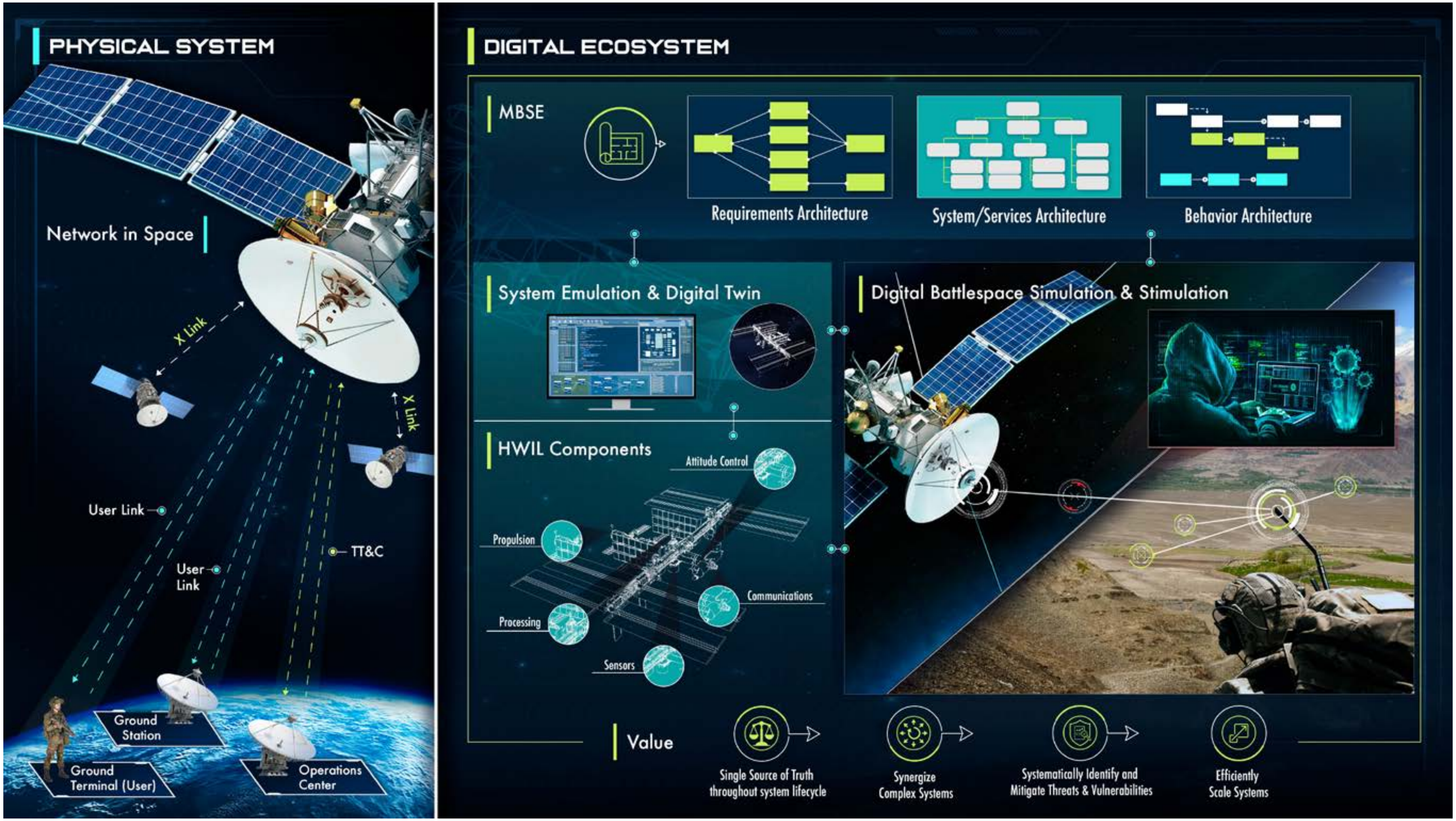
Maritime



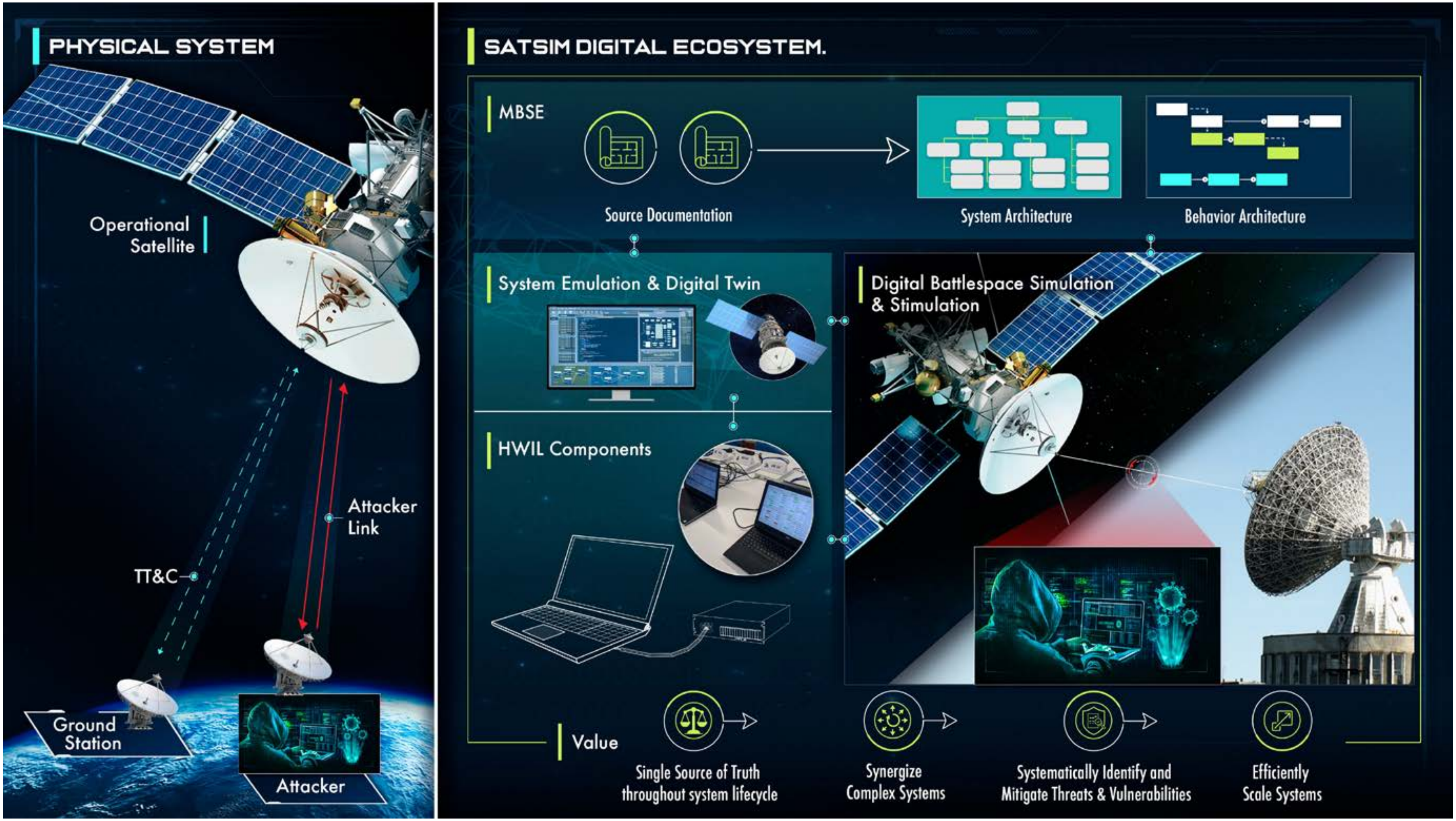
Building & Site Management

Industrial Control Systems

SPACE DIGITAL ECOSYSTEM


PHYSICAL SYSTEM
Network in Space
X Link
X Link
User Link
User Link
TT&C
Ground Station
Ground Terminal (User)
Operations Center
DIGITAL ECOSYSTEM
MBSE
Requirements Architecture
System/Services Architecture
Behavior Architecture
System Emulation & Digital Twin
Digital Battlespace Simulation & Stimulation
HWIL Components
Attitude Control
Propulsion
Processing
Communications
Sensors
Value
Single Source of Truth throughout system lifecycle
Synergize Complex Systems
Systematically Identify and Mitigate Threats & Vulnerabilities
Efficiently Scale Systems

SATSIM FOCUS AREA: CONTROL SEGMENT


PHYSICAL SYSTEM
Operational Satellite
Attacker Link
TT&C
Ground Station
Attacker
SATSIM DIGITAL ECOSYSTEM.
MBSE
Source Documentation
System Architecture
Behavior Architecture
System Emulation & Digital Twin
Digital Battlespace Simulation & Stimulation
HWIL Components
Value
Single Source of Truth throughout system lifecycle
Synergize Complex Systems
Systematically Identify and Mitigate Threats & Vulnerabilities
Efficiently Scale Systems

SATSIM: GPS DIGITAL TWIN

Our Government client tasked Booz Allen Hamilton with addressing a list of potential cyber vulnerabilities in legacy GPS systems.

Requirements

- Deadline of 11 months from initial ask to final report
- Had access only to ICDs and design documents
- Needed to show convincing proof or disproof of test objectives

Results

- Team built a digital twin of the ground station, satellite bus and control link in 6 months
- Performed all testing in required timeline
- Uncovered additional items of interest
- Suggested remedies that are currently in use

EXECUTION OPTIONS

The team identified multiple paths to fulfilling the requirements, each with some inherent risk.

On-Orbit Satellites

- No, just no

Test Platform / Flat Sat

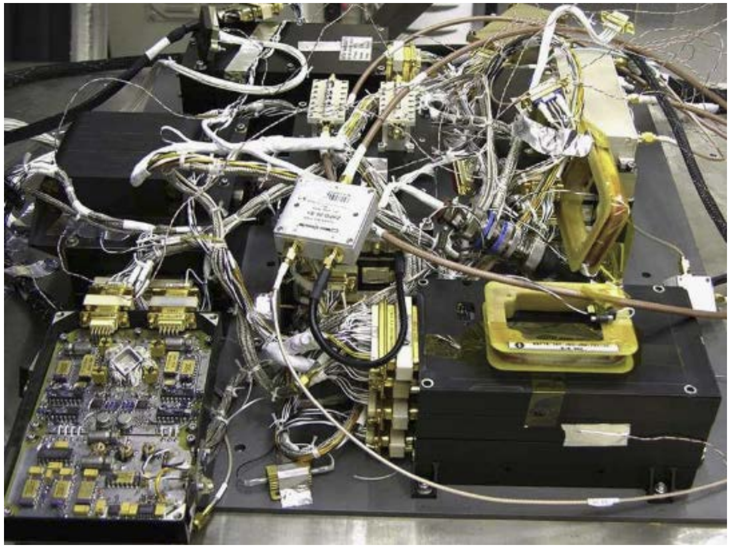
- Secured facility
- No guarantee of access within deadline
- No guarantee of ATO
- Risks de-certifying test equipment

Paper-based Assessments

- Low cost
- Do not directly demonstrate issues
- Do not support “creative” testing
- Relies on individuals, not fungible

Software Model / Digital Twin

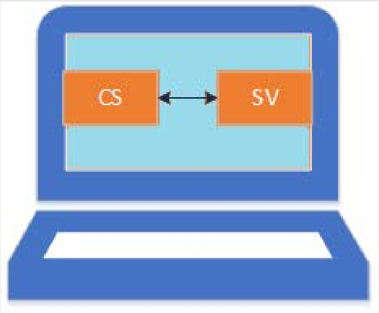
- Requires development time
- Reasonable fidelity
- Superior flexibility
- Transportable



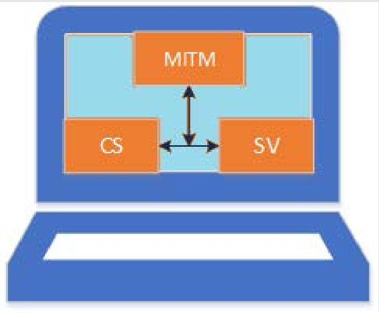
OPERATIONAL MODES

Development / Demonstration

Control Segment + Space Vehicle

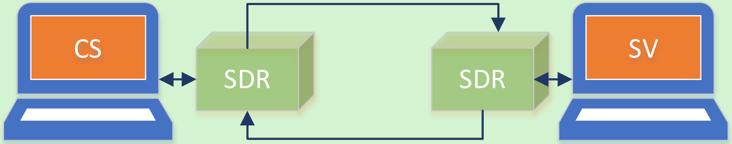


CS + SV + Man in the Middle (MITM)

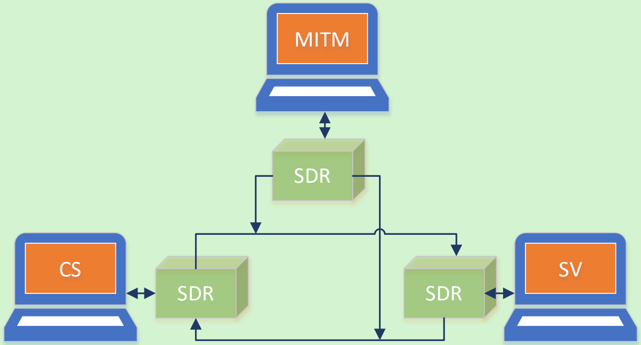


Test / Validation

CS + SV over radio



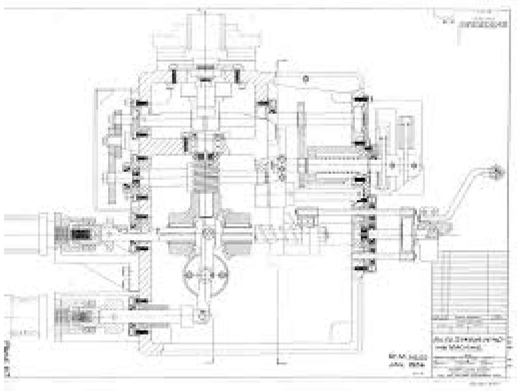
CS + SV + MITM over radio



(CS = Control Station, SV = Space Vehicle, MITM = Man in the Middle)

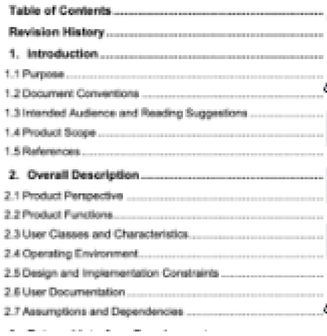
PROCESS: DOCUMENT REVIEW

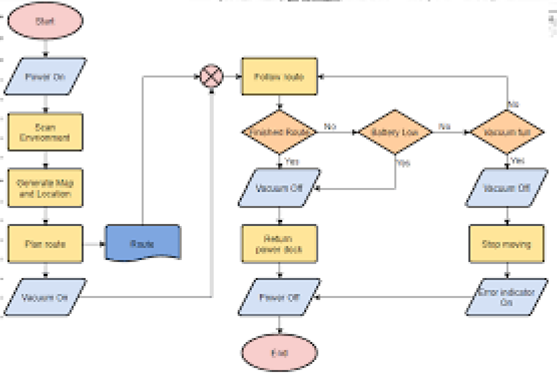
To understand the entire system, the team reviewed thousands of pages of documents spanning dozens of revisions over 20 years



Functional Requirements

Requirement ID	Requirement Statement	Must/Want	Comments
FR001	[illegible]	Must	
FR002	[illegible]	Must	
FR003	[illegible]	Must	[illegible]
FR004	[illegible]	Must	[illegible]
FR005	[illegible]	Must	[illegible]
FR006	[illegible]	Must	[illegible]

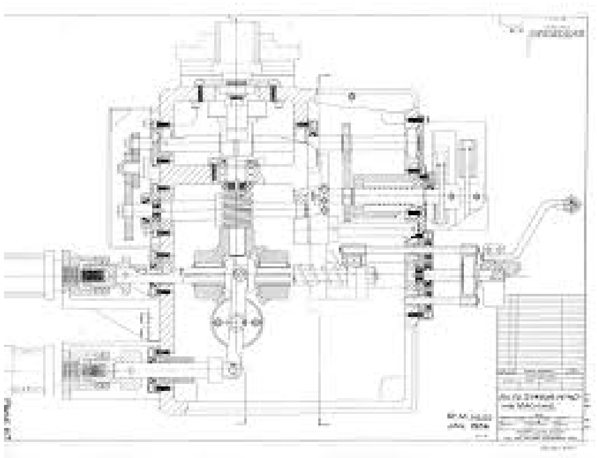




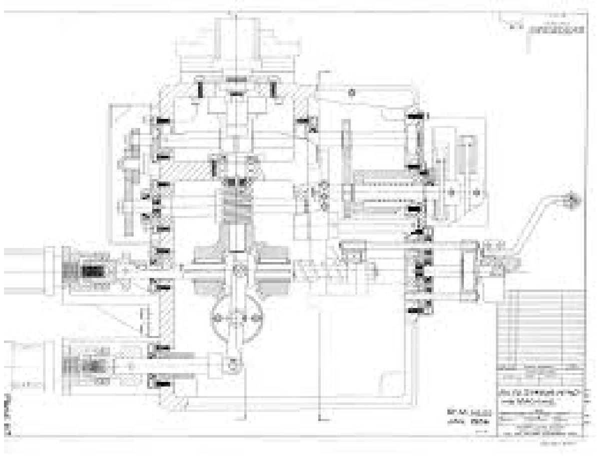
PROCESS: MORE DOCUMENT REVIEW

This documentation, while complete, was not always consistent

- Uncovered several notable inconsistencies between documents
- Led to some uncertainty as to component design
- Institutional knowledge loss
- On-Orbit Handbook (OOH) was tie-breaker

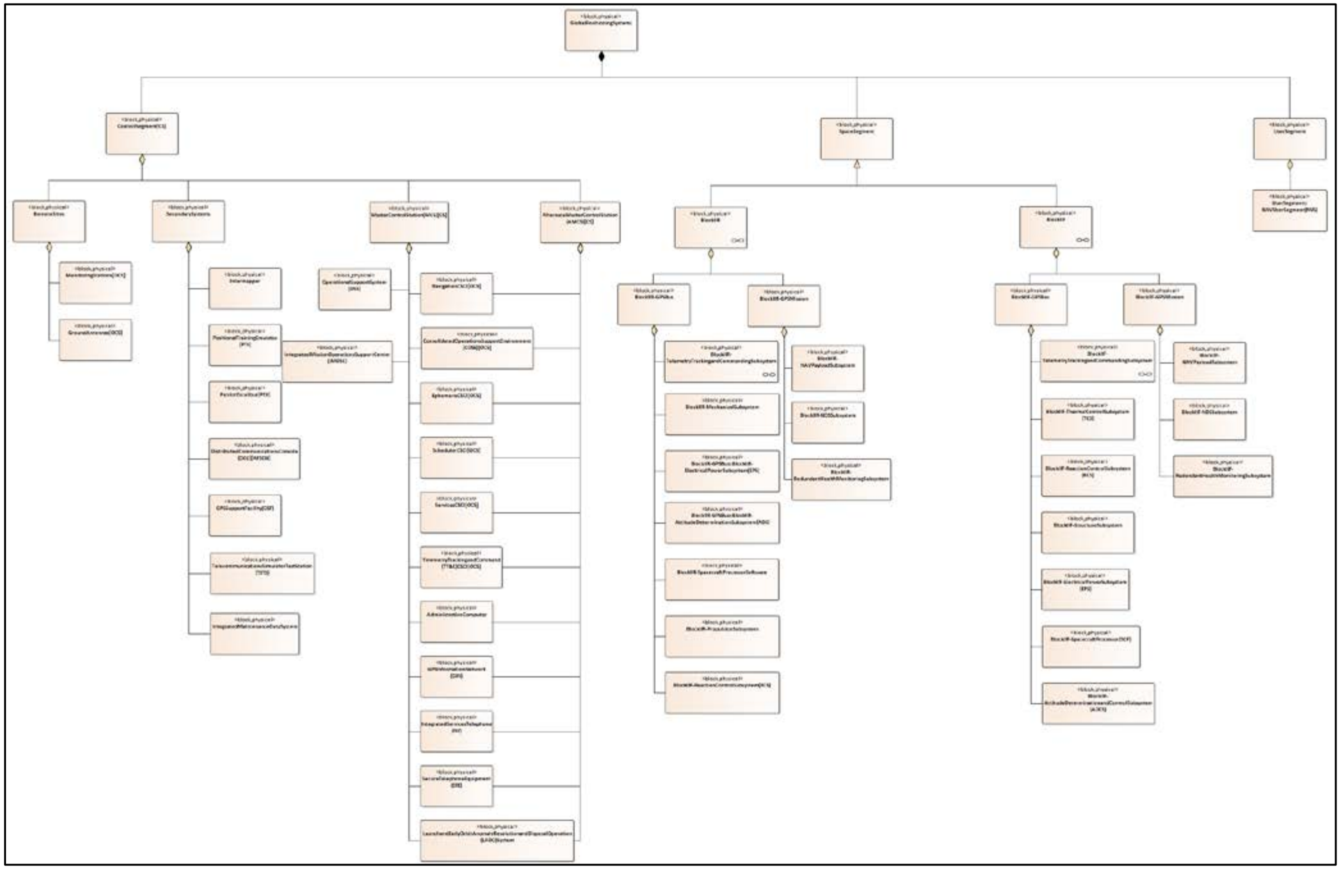


≠

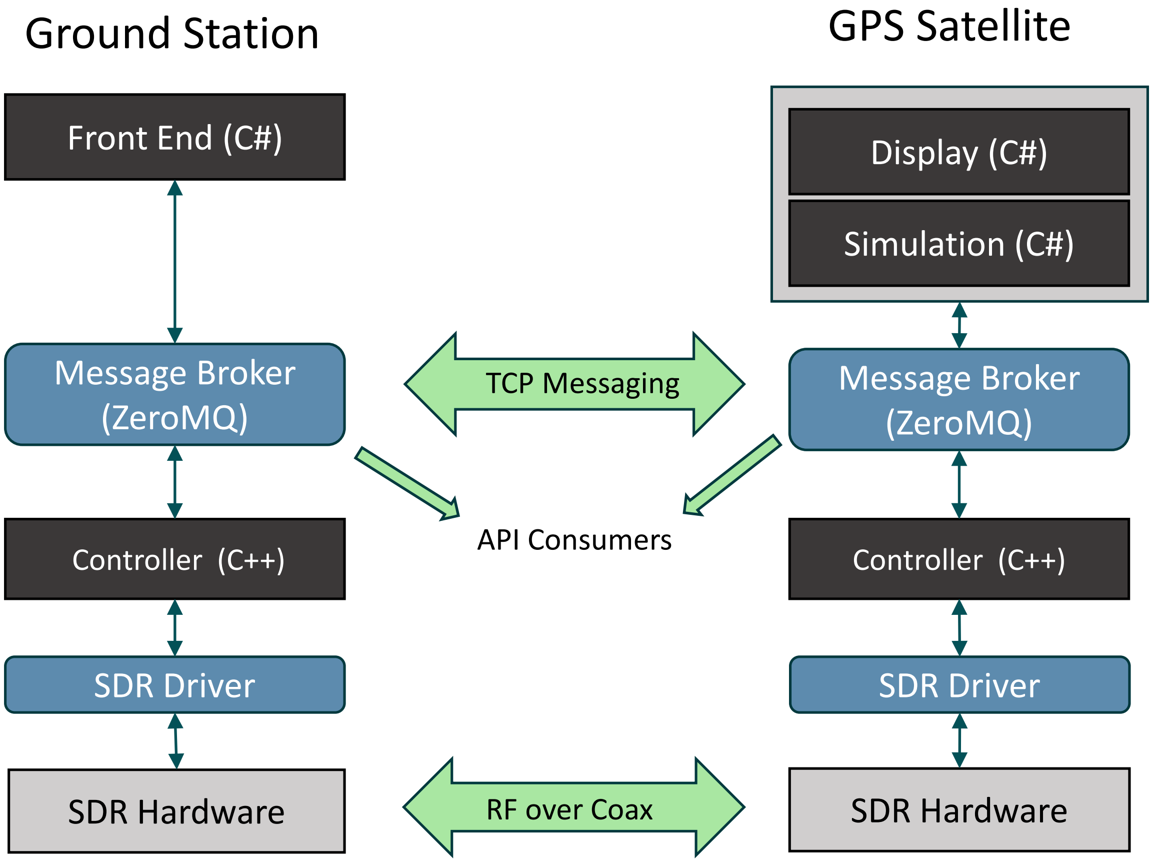


DIGITAL ENGINEERING (MBSE) MODEL

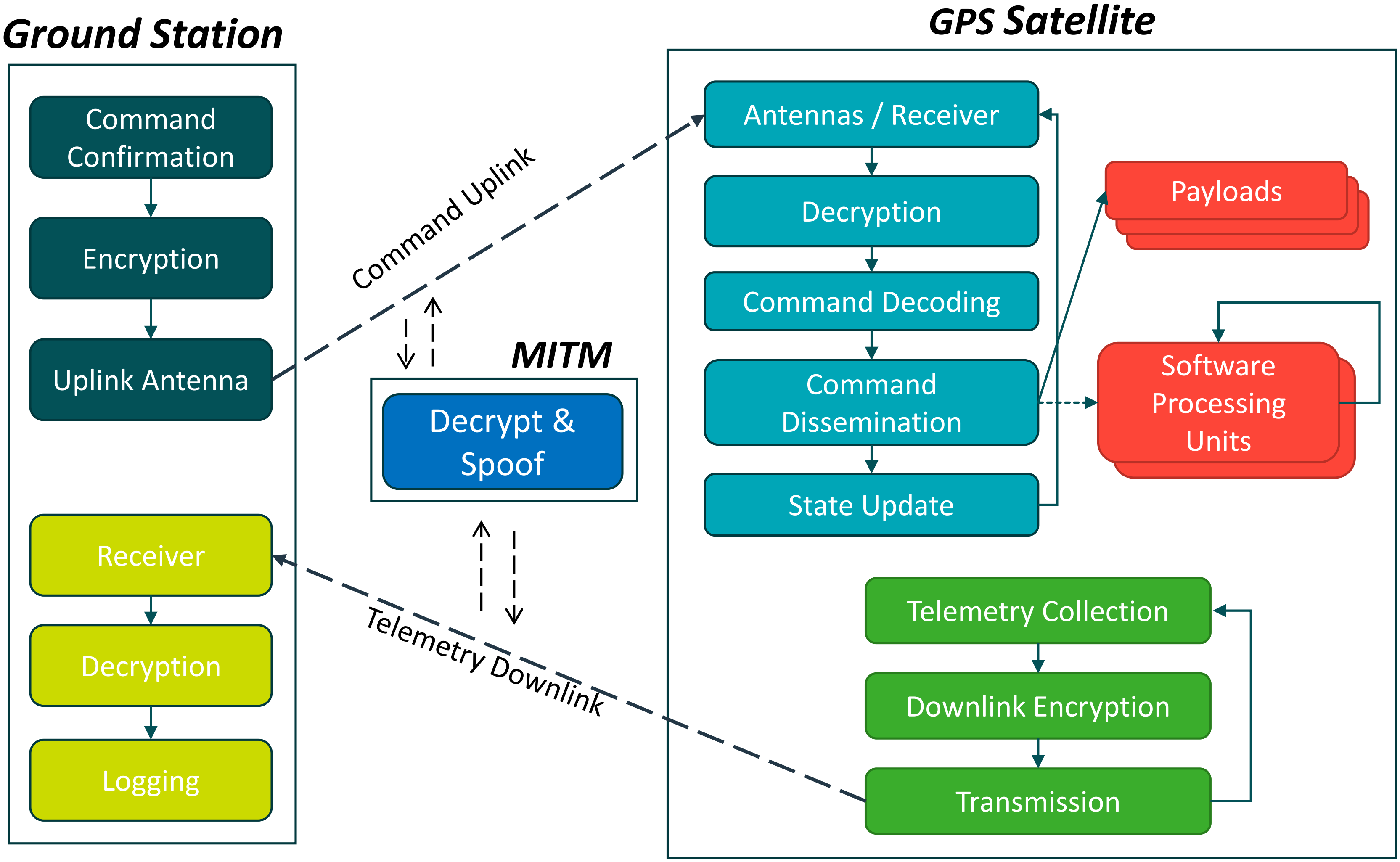
Building on this knowledge, we developed a descriptive MBSE model to further shape the project requirements and inform stakeholders.



APPLICATION ARCHITECTURE



FUNCTIONAL ARCHITECTURE



RESULTS

Developed over six months from ICDs and procedural documents, SatSim emulates the ground control link and satellite bus to probe cybersecurity issues.

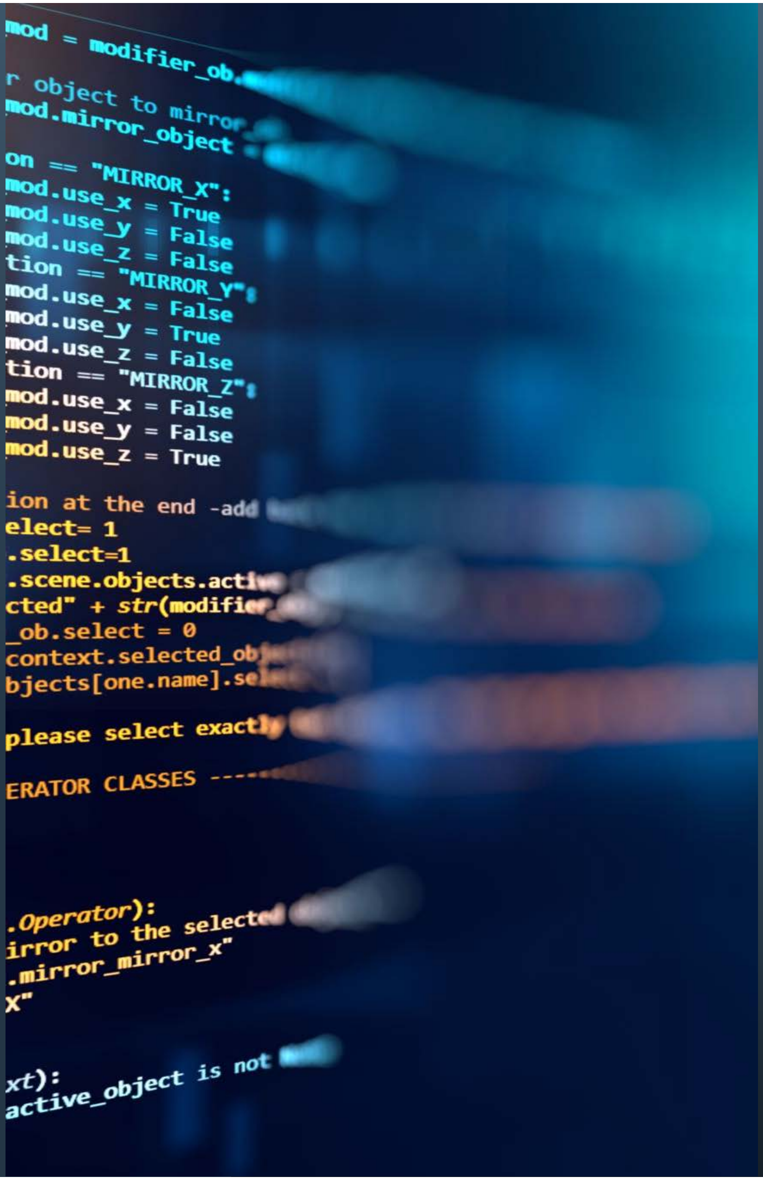
Outcome

- Identified inconsistencies and errors in documentation
- End-to-end approach discovered vulnerabilities and remediations not considered by the system developer
- **Performed and validated all test items without risking full-scale or test systems**

Extended Uses

- Flexible environment for testing
- Training environment
- Validate tactics, tools and procedures
- Function as stand-in for real test platform

SatSim testing in SDR mode



```
mod = modifier_ob
r object to mirror
mod.mirror_object
on == "MIRROR_X":
mod.use_x = True
mod.use_y = False
mod.use_z = False
tion == "MIRROR_Y":
mod.use_x = False
mod.use_y = True
mod.use_z = False
tion == "MIRROR_Z":
mod.use_x = False
mod.use_y = False
mod.use_z = True

ion at the end -add
elect= 1
.select=1
.scene.objects.active
cted" + str(modifier
_ob.select = 0
context.selected_ob
bjects[one.name].se

please select exactly

ERATOR CLASSES ----

.Operator):
irror to the selected
.mirror_mirror_x"
x"

xt):
active_object is not
```

CYBER PHYSICAL TESTBEDS (CPT)

FUCHEE VANG

AGENDA

- Mission
- Purpose
- Training and Exercises
- Testbeds overview

MISSION

CPT provides Cyber Operators with full-spectrum, multi-domain cyber education, training, exercises, and experimentation capabilities utilizing tradecraft tailored to direct mission sets.

PURPOSE

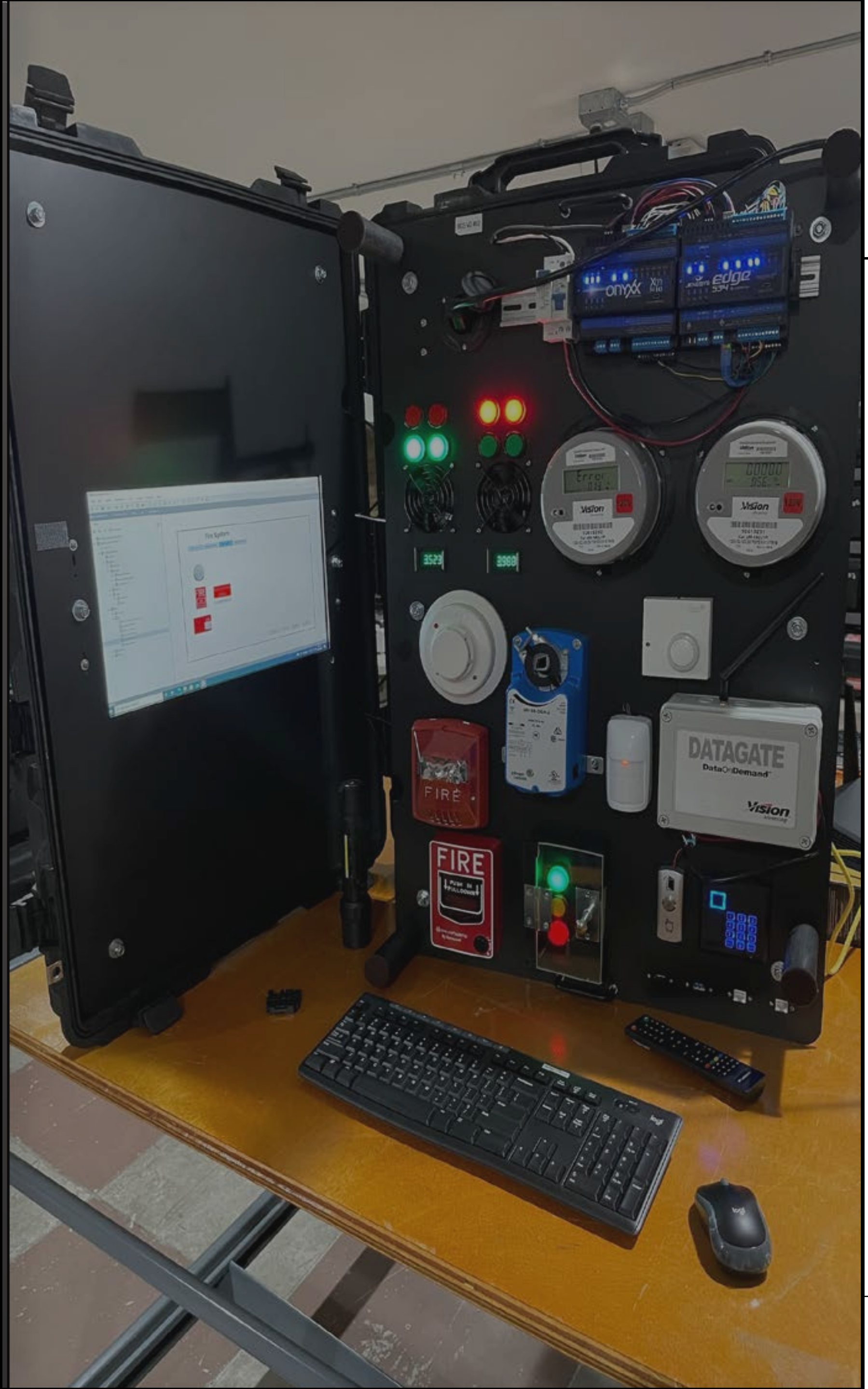
PROVIDE SUPPORT TO THE DEVELOPMENT OF AN ORGANIC CYBER FORCE VIA STRATEGY, DOCTRINE, STANDARDS DEVELOPMENT, TRAINING, EDUCATION, AND EXERCISES:

- Strategy, Doctrine, and Standards Development
  - Formalizing training standards and developing KSAs for tactical cyber operations
- Training, Education and Exercises
  - Cyber Physical Testbeds (CPT)
  - ACPT

TRAINING EDUCATION AND EXERCISES CONCEPT OF OPERATIONS

CYBER PHYSICAL TESTBEDS ENABLE:

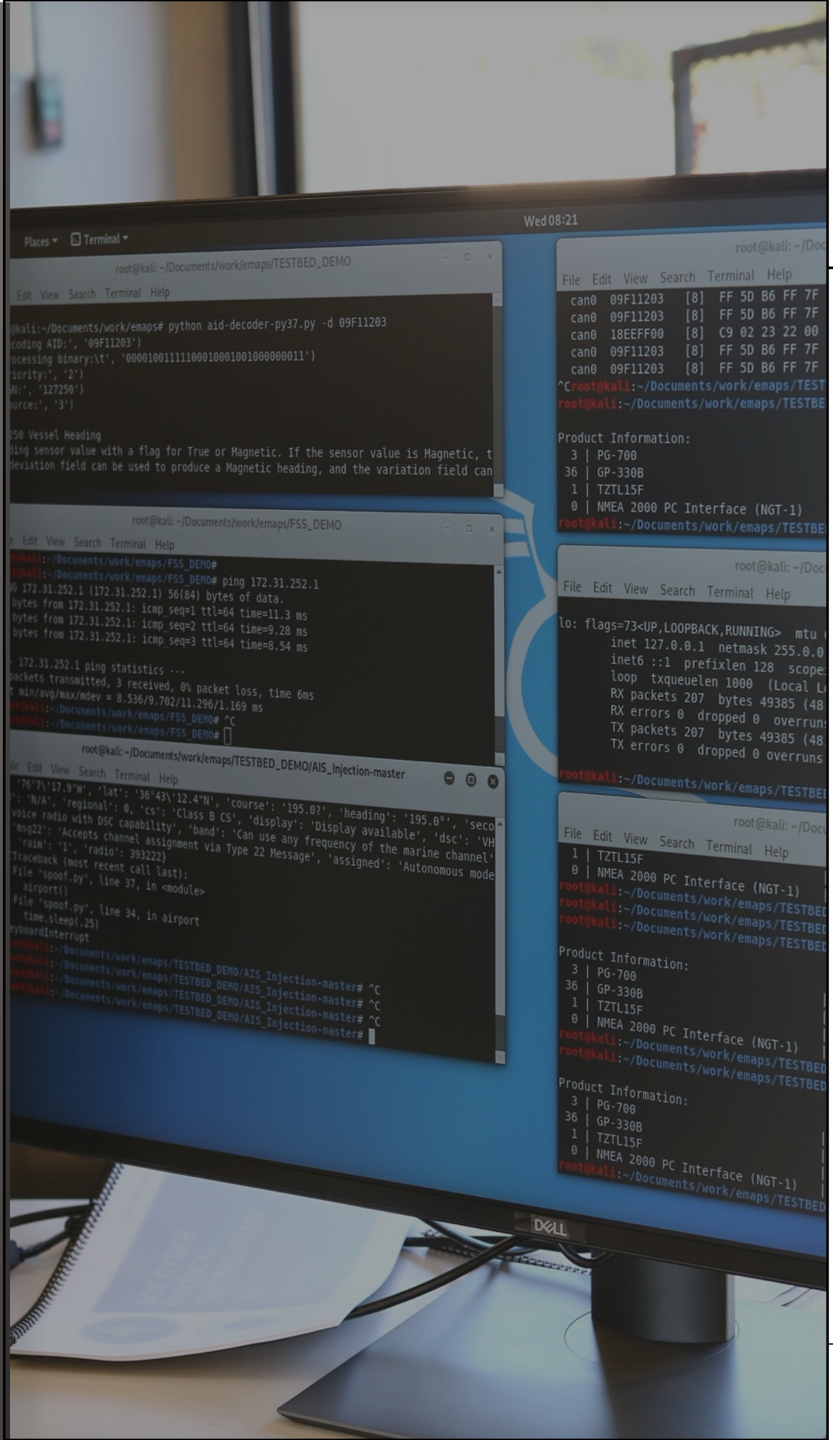
- Conduct FTXs with the joint force enabling peculiar mission sets.
- Conduct mission rehearsal on realistic replications of real-world systems utilizing AOR specific protocols.
- Test and validate offensive and defensive cyber capabilities.
- DEVOPS capability for cyber requirements.



CYBER PHYSICAL TESTBEDS (CPT)

REAL NOT VIRTUAL INSTANTIATIONS OF CYBER ENVIRONMENTS:

- The benefits of being able to conduct training/mission rehearsals and capability development using physical instantiations, vice virtual are numerous: realism, normalization of cyber operations, more rapid capability development/validation, tactile response (effects can be seen in the environment immediately), and talent retention (the more realistic the training, the higher the retention).



CPT, TRAINING AND EXERCISES CONCEPT OF OPERATIONS

- An event consists of Cyber Exercise Planners, On Site Engineers and the Testbed Build Team to achieve stated goals and objectives.
- Cyber Exercise Planners will attend events, conduct storyline development, script injects, Master Scenario Event List (MSEL) management, and AAR development.
- Testbed Engineers will coordinate the configuration and management of technical aspects of the cyber physical testbeds to support exercise development and training.
- Build team ensures that testbeds are functional and ready for deployment during any given exercise.

EXPLOIT DEVELOPMENT AND TRAINING

- Testbed Engineers will deliver a comprehensive training guide that will walk cyber teams through exercises and operation of the cyber physical testbed.
- Testbed Engineers will deliver onsite training catered to the skill level of cyber teams
- Programming documentation and scripts will be provided to enable further development of exploits beyond on-site coursework
- Curriculum includes (but not limited to)

Maritime Control System

- Reconnaissance/ scanning
- Enumeration of network
- Exploitation and more enumeration
- Spoofing AIS Data
- AIS Injection
- Triggering Vessel Collision Alarm
- Disabling a Device
- Walkthrough of each exploitation techniques

Building Control System

- Reconnaissance/scanning
- Enumeration of network
- Exploitation port power shutdown
- Remote system access
- Control of central user interface which controls locks, alarms, and motion detectors

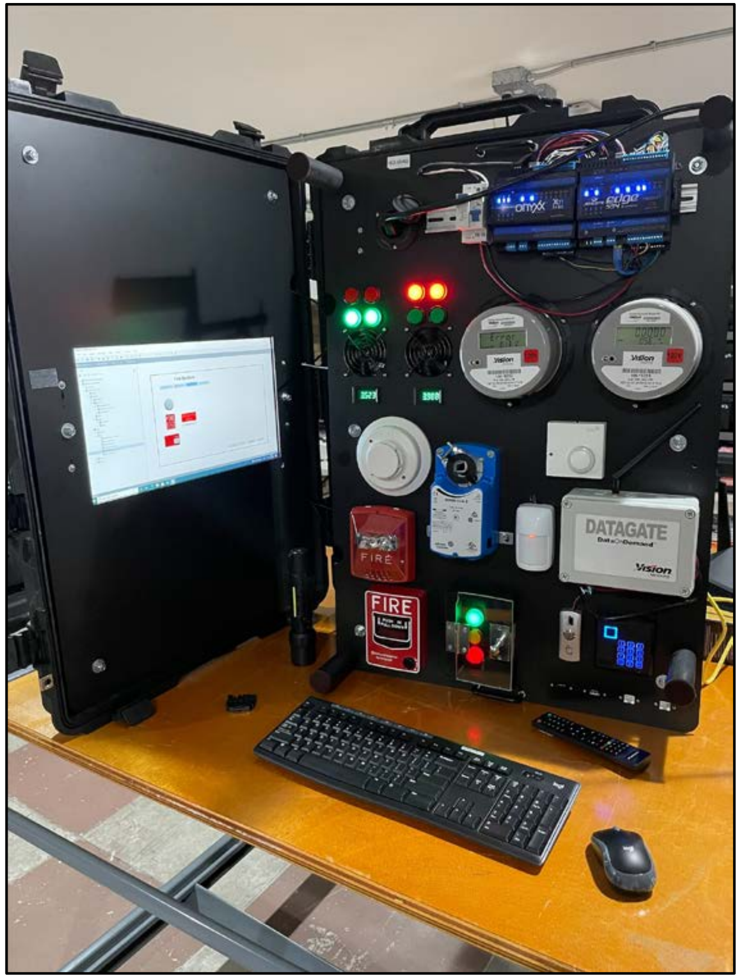
Building Surveillance System

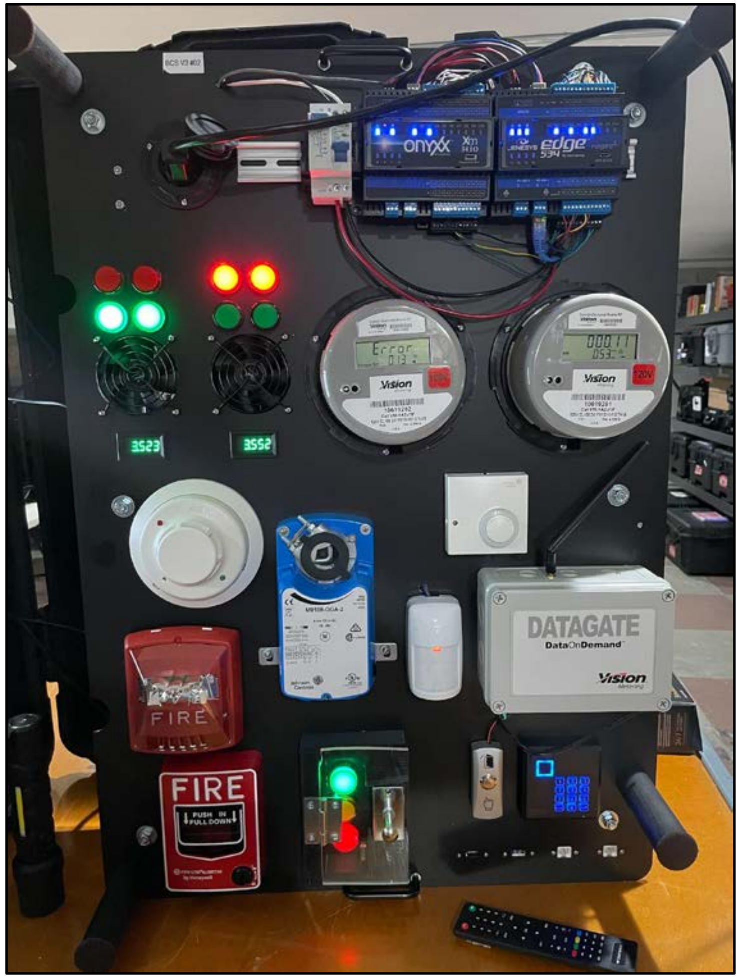
- Reconnaissance/scanning
- Enumeration of network
- Denial of service
- Freezing camera feeds
- Remote access to camera feeds
- Close access user password reset

Cell Tower on Wheels

- Reconnaissance/scanning
- Enumeration of network
- Denial of service
- Remote system access/pivoting
- Control of central user interface (server core and ecx manager)

BUILDING CONTROL SYSTEM (BCS)





- Replicates building control and access systems used in commercial building domains integrating commercial off-the-shelf products in a transportable cyber physical testbed.
- Version 3 uses only one display screen along with increased ruggedization construction.

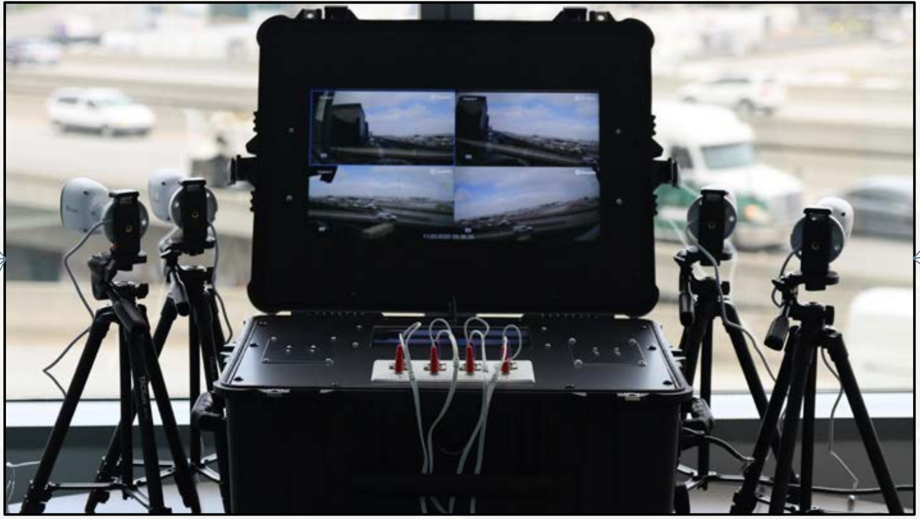
BUILDING SURVEILLANCE SYSTEM (BSS)

COTS WiFi enabled CCTV DVR Surveillance System

Wired CCTV Cameras

Wireless IP Cameras*

Cloud enabled wireless cameras*



COTS Network Switch

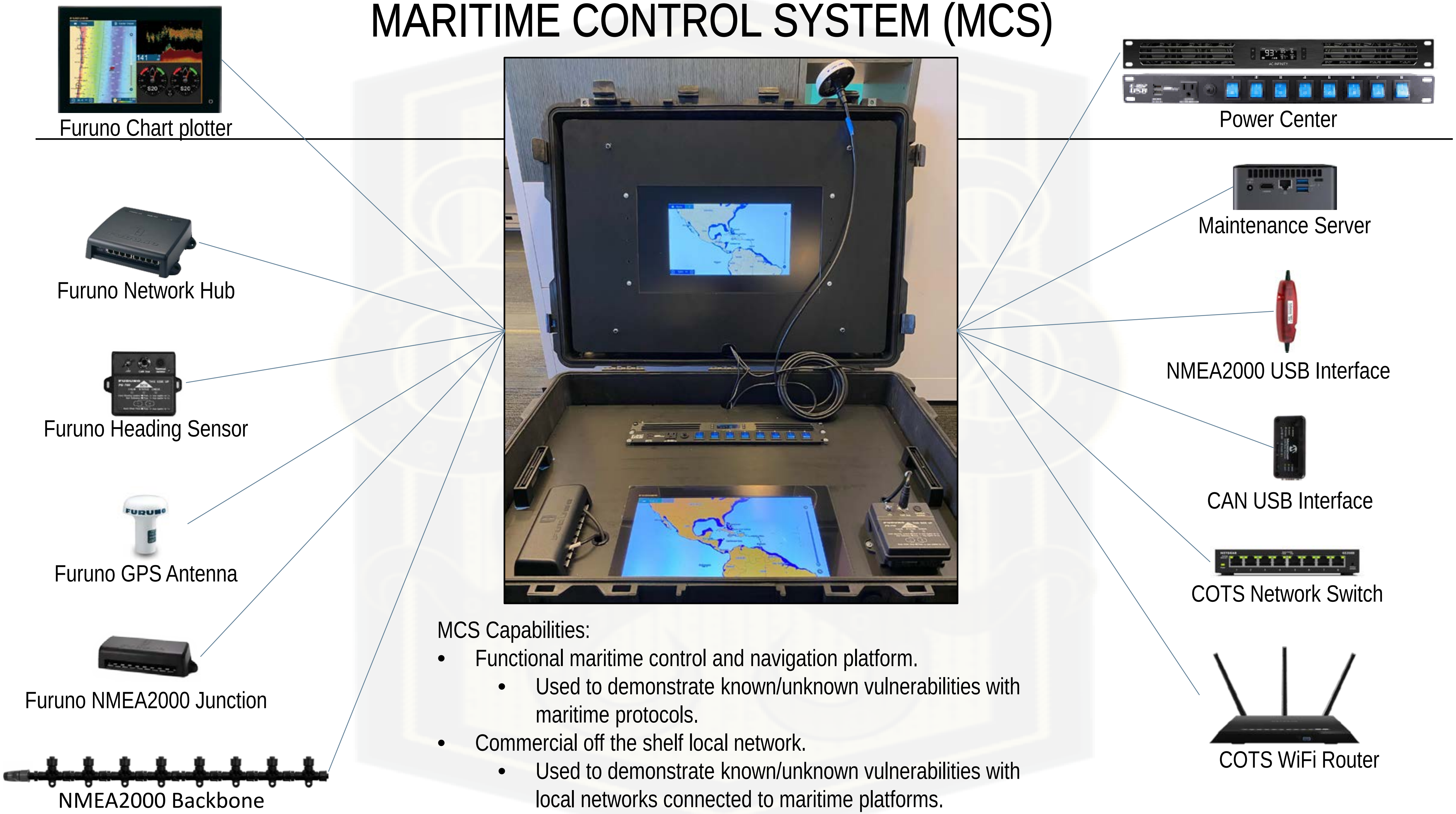
COTS WiFi Router

Media Server*

BSS Capabilities:

- Functional video surveillance platform.
  - Used to demonstrate known/unknown vulnerabilities with video surveillance protocols.
- COTS local network.
  - Used to demonstrate known/unknown vulnerabilities with local networks connected to video surveillance equipment.

MARITIME CONTROL SYSTEM (MCS)



Furuno Chart plotter

Furuno Network Hub

Furuno Heading Sensor

Furuno GPS Antenna

Furuno NMEA2000 Junction

NMEA2000 Backbone

Power Center

Maintenance Server

NMEA2000 USB Interface

CAN USB Interface

COTS Network Switch

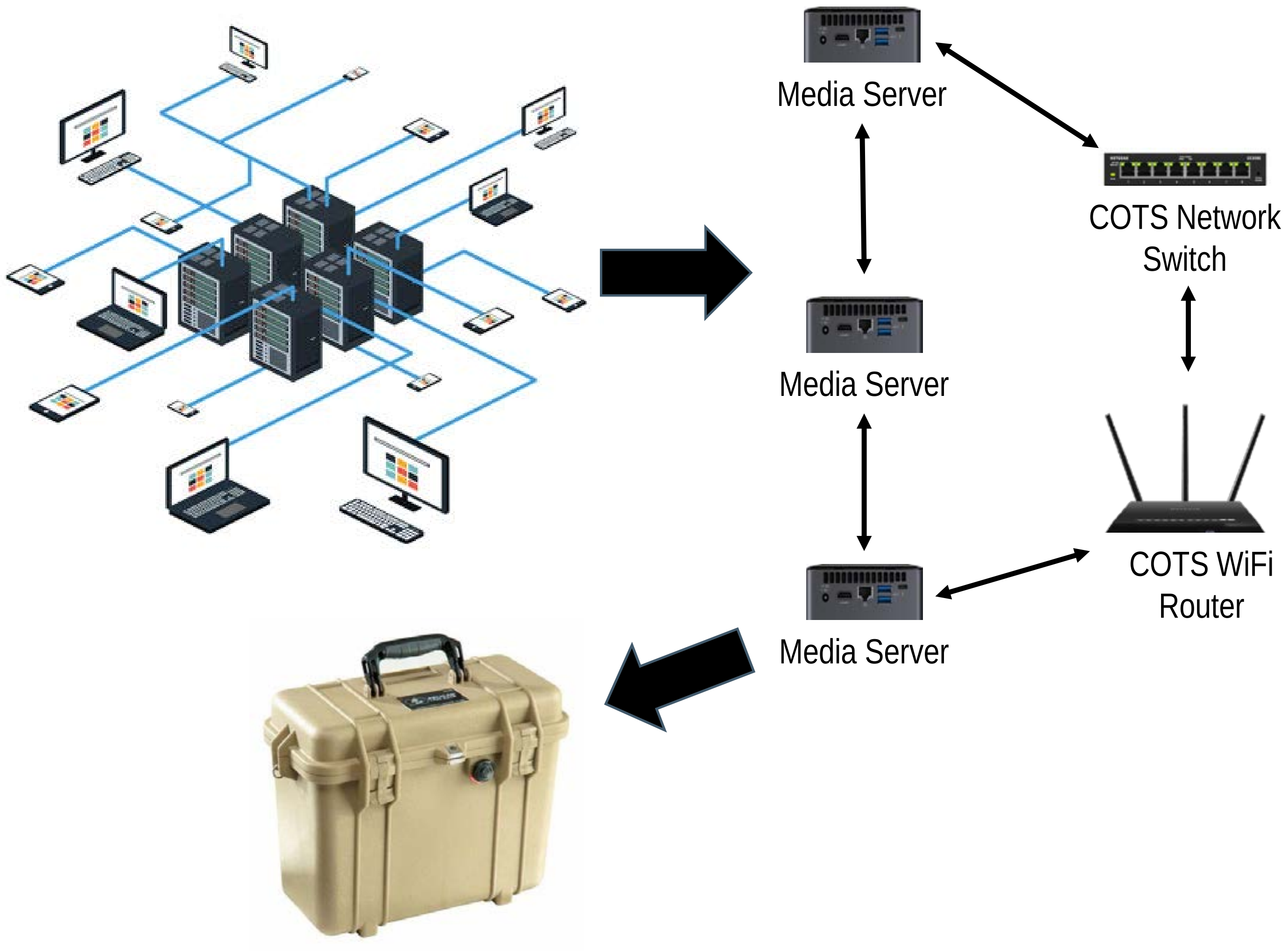
COTS WiFi Router

MCS Capabilities:

- Functional maritime control and navigation platform.
  - Used to demonstrate known/unknown vulnerabilities with maritime protocols.
- Commercial off the shelf local network.
  - Used to demonstrate known/unknown vulnerabilities with local networks connected to maritime platforms.

CORPORATE STYLE NETWORK (CSN)

- Employed to facilitate exercises worldwide
- Simulates an enterprise's communications backbone that connects computers and related devices
- Enables exploitation and enumeration of an adversarial network
- Simulate’ s X# of virtualized systems to create a realistic Corporate Style Network
- No lithium-ion batteries incorporated into the design to avoid scrutinization by air carriers



VEHICLE CONTROL SYSTEM (VCS)

- <u>Expected Capabilities:</u>
- Exploits weak cryptographic management
- Utilizes vulnerabilities in head unit firmware, TCU firmware, and telecom infrastructure
- Physical access to vehicle unnecessary
- Capable of remotely executing telematics protocols:
  - Remote Start
  - Remote Lock/Unlock
  - Electric Ignition Control
  - Geolocation
  - Anti-Theft
  - Emergency Calling
- Transported in small Pelican case