Creating a Virtual Ship Environment Optimized for Cybersecurity Use

Presented by:

Jeff Greer , Asst. Professor of Practice in Cybersecurity @ UNCW

Laavanya Rachakonda (PhD), Asst. Professor Computer Science @ UNCW

Hosam Alamleh (PhD), Asst. Professor Computer Science @ UNCW

Joint Study Partners

- State university located in Wilmington, NC
- Center for Cyber Defense Education
- MCARTEC Research Hub
- Specialized Maritime Cybersecurity classes
- Principal investigator
  - Jeff Greer
- Supporting research team being formed

- Supplier of marine technology located in Gdynia, Poland
- Offering state of the art marine engine simulators for merchant seaman education and assessment
- Study sponsors:
  - Dr. Kluj, Founder
  - Rafal Pawletko, Technical Director

System of Interest (SOI)

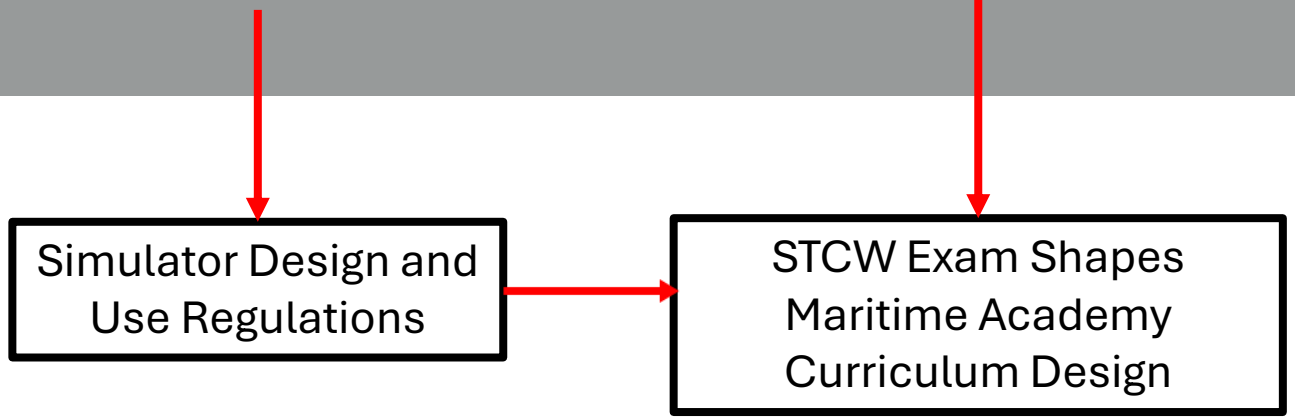


Simulator Design Shaped by Training Need and Regulatory Compliance

To meet the requirements:

Engine Room Simulator has been developed to comply with STCW Code:

- Section A-1/12 and Section B-1/12
- ISM Code: Section 6 and Section 8



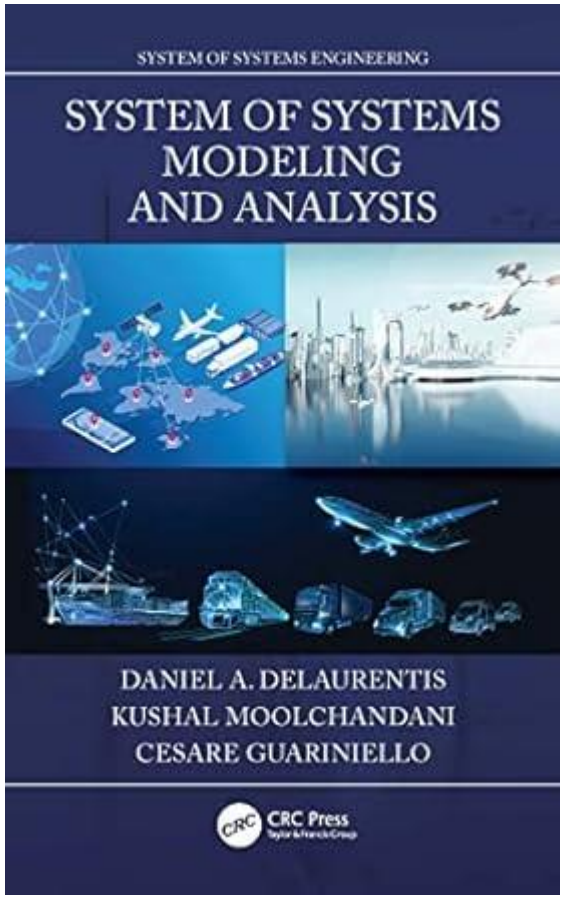
Alternate Use Case (UC) Study - Applied Cybersecurity

- UC 1 - Simulator use for teaching ship domain knowledge to cybersecurity students who are non mariners
- UC 2- Simulator use for teaching security by design using MBS2E concepts
- UC 3 - Simulator use for teaching and assessing student response to relevant cyber-attack scenarios

Study Methodology

UC #	Educational Need	Use Case Simulator Functional Requirements	Current Simulator Functional Capabilities	Identified Simulator Functional Improvements
1	Ship domain knowledge			
2	Cyber risk management strategy design			
3	Cyber-attack incident response			

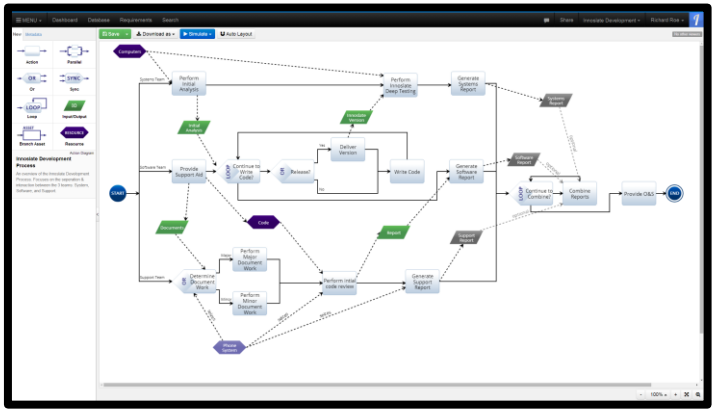
Supplemental Study Material and Tools



Notion of MBS2E

SPEC INNOVATIONS

Study Sponsor



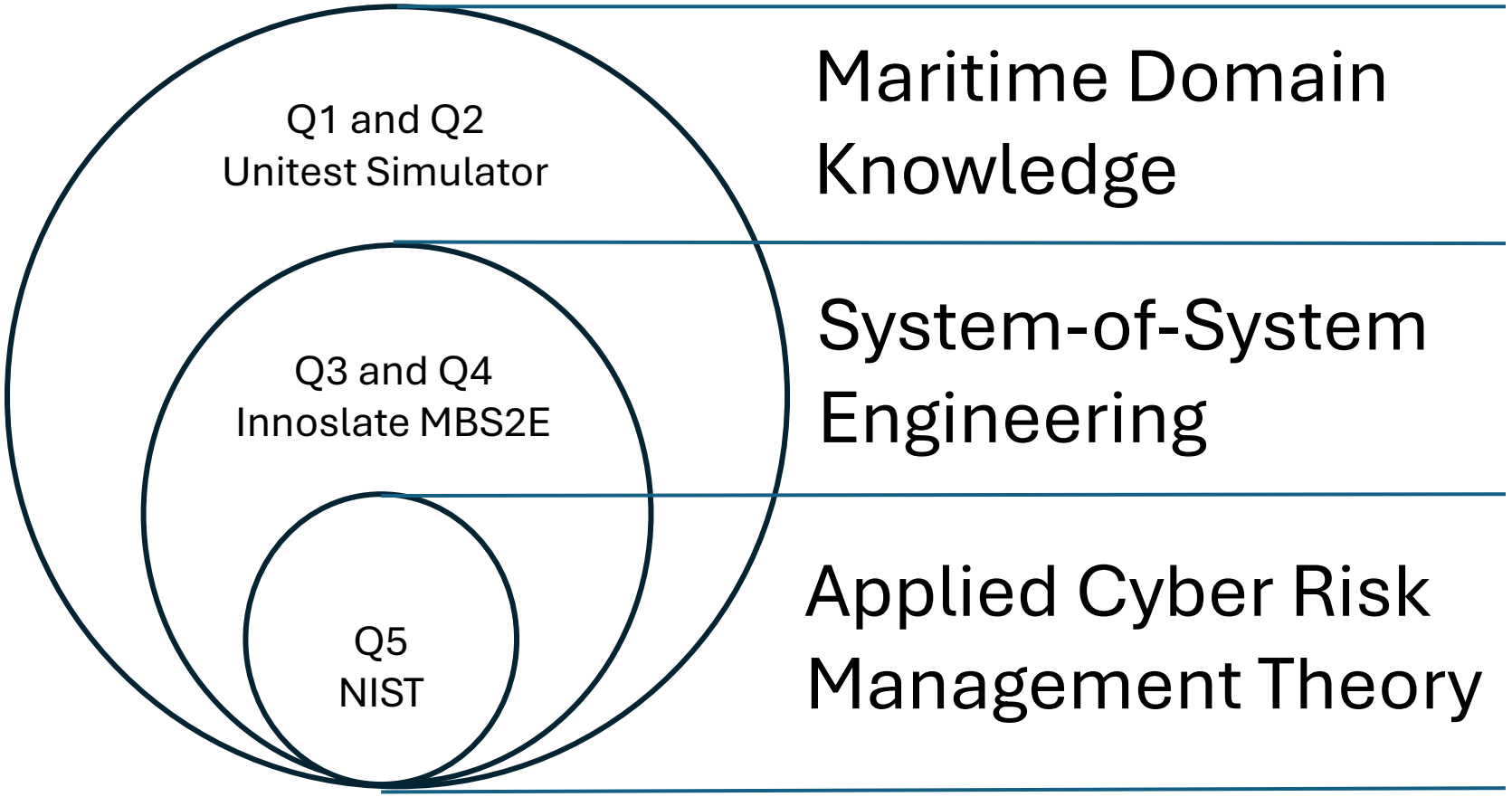
Innoslate – Cloud MBSE Application

Cybersecurity Education Simplified

	Varying Role-based Educational Needs	
5 Critical Thinking Skills	**Student**	**Industry Employee**
1. What is it?	?	NA
2. Why is it important?	?	NA
3. How does it work? (1)	?	?
4. How can it fail?	?	?
5. How can failure be prevented	?	?

Note (1) – system-of-systems, discrete systems, and components

UNCW Transdisciplinary Education Approach



Unitest X92 Simulator

Winterthur Marine Gas & Diesel (G&D) Engine

SOI - Stereotypical Ship

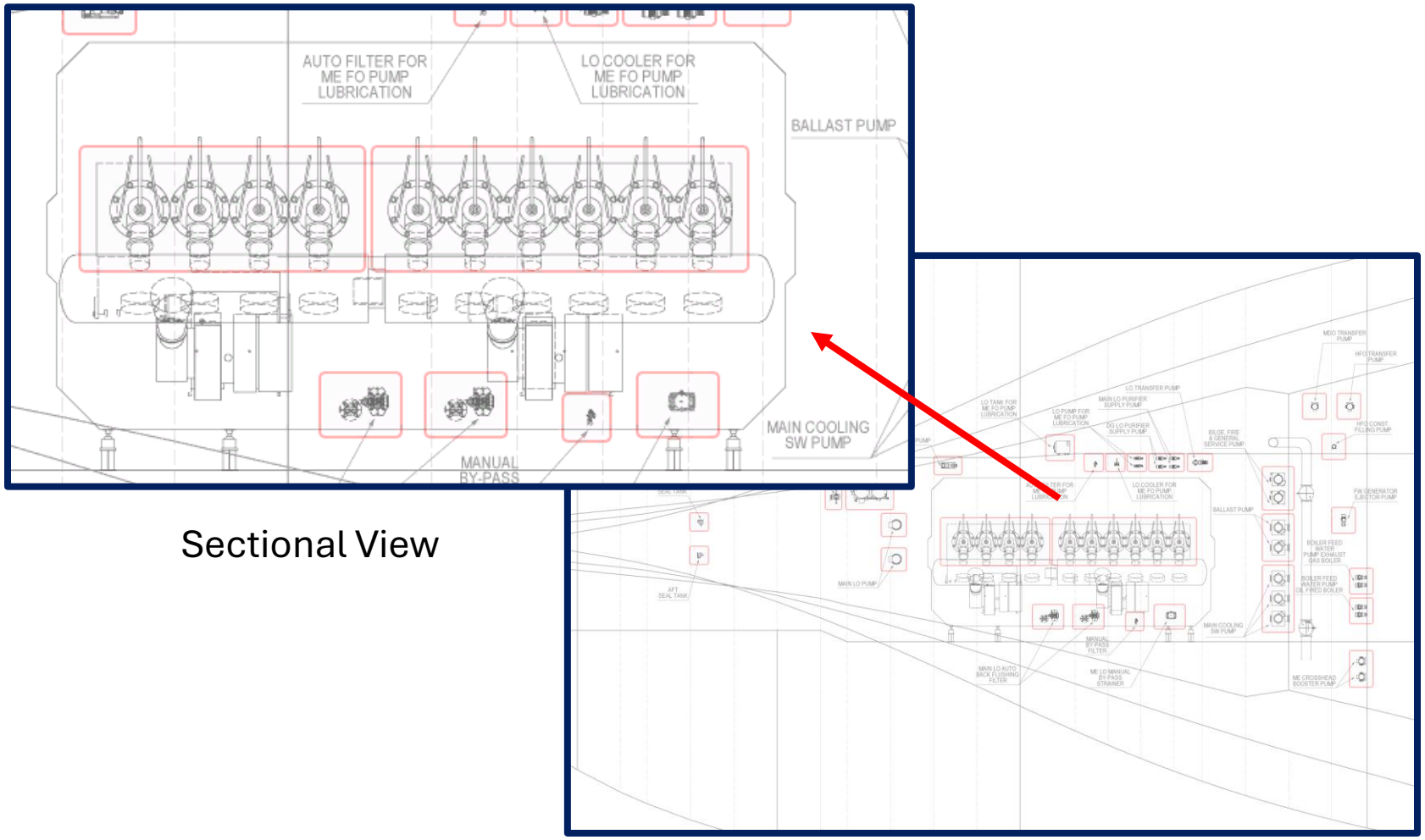


Container Ship	Characteristics
Engine Room Type	Low Speed
Length	366 m
Width	49 m
Max Speed	22kn
Dead Weight	148,992 t
Gross Tonnage	140,872 t
TEU	14,400

Ship – an Apex Cyber Physical System With 20 Subsystems

- Bridge
- Diesel Generator
- Emergency Generator
- Main Engine
- Compressed Air System
- Cooling System
- Lubricating System
- Fuel System
- Steam System
- Ballast System
- Steering Gear System
- Bilge System
- Steering Gear
- CO2 Fire Extinguishing System
- FW & Sanitary Water System
- Stern Tube Seal
- Sewage Treatment Plant
- Refrigeration Plan
- AC Plant
- Incinerator

Deck Plans – Subsystem Locations



Sectional View

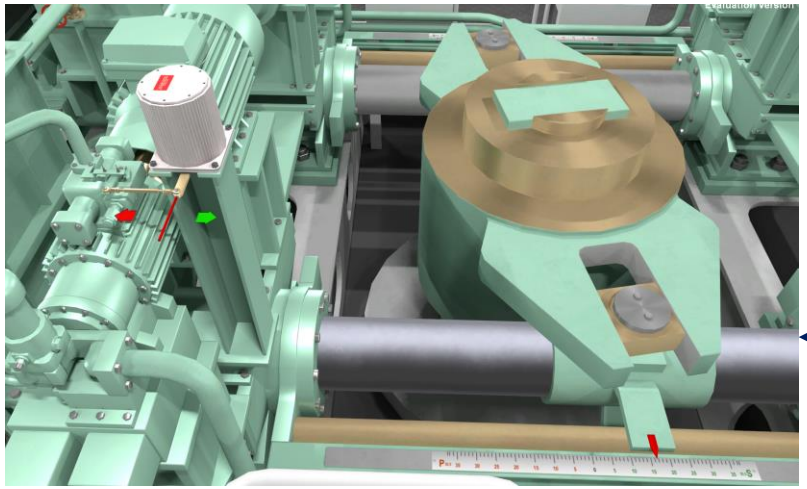
Bridge – Engine Ctrl. Room Coms.

Bridge





Helm

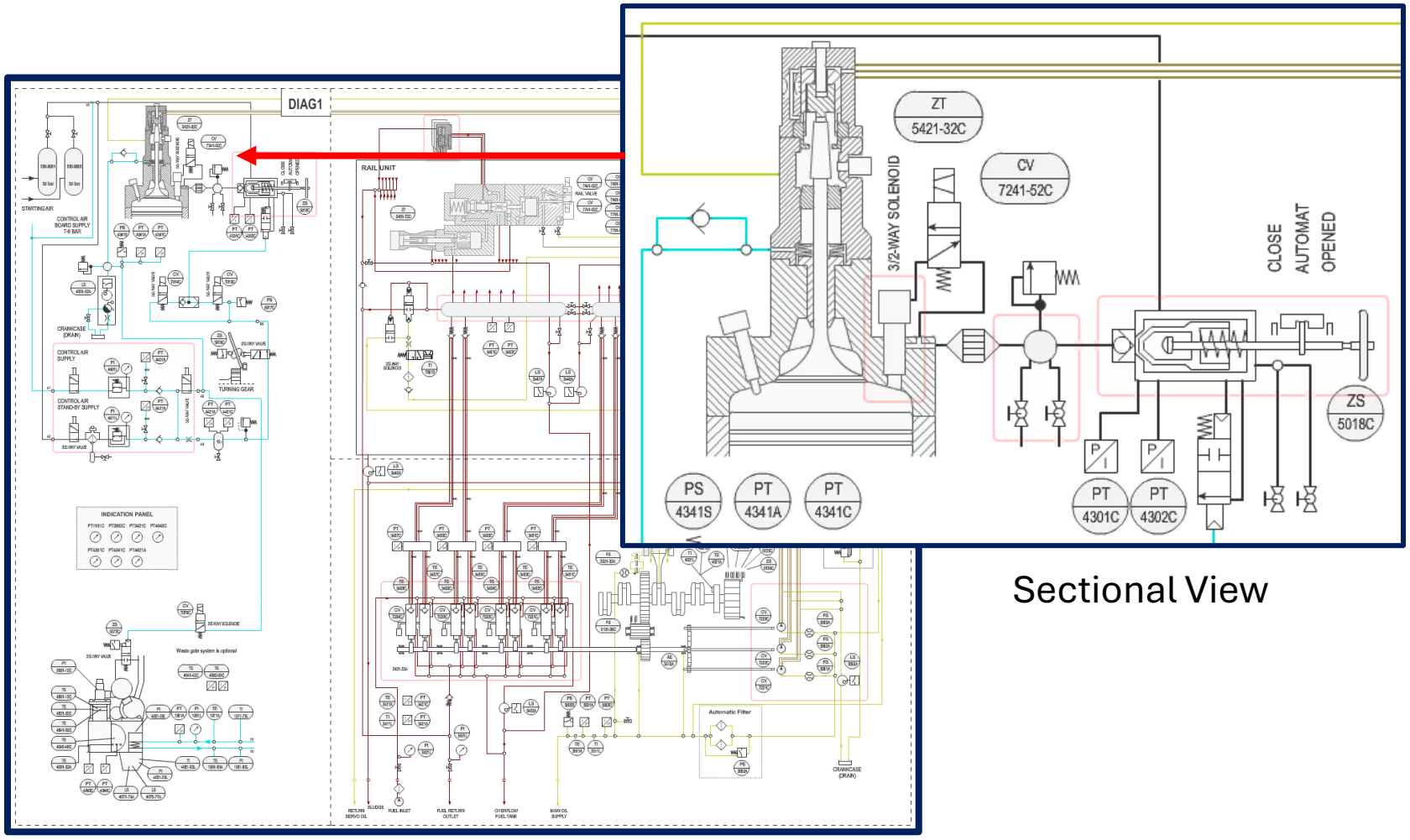


Steering Gear

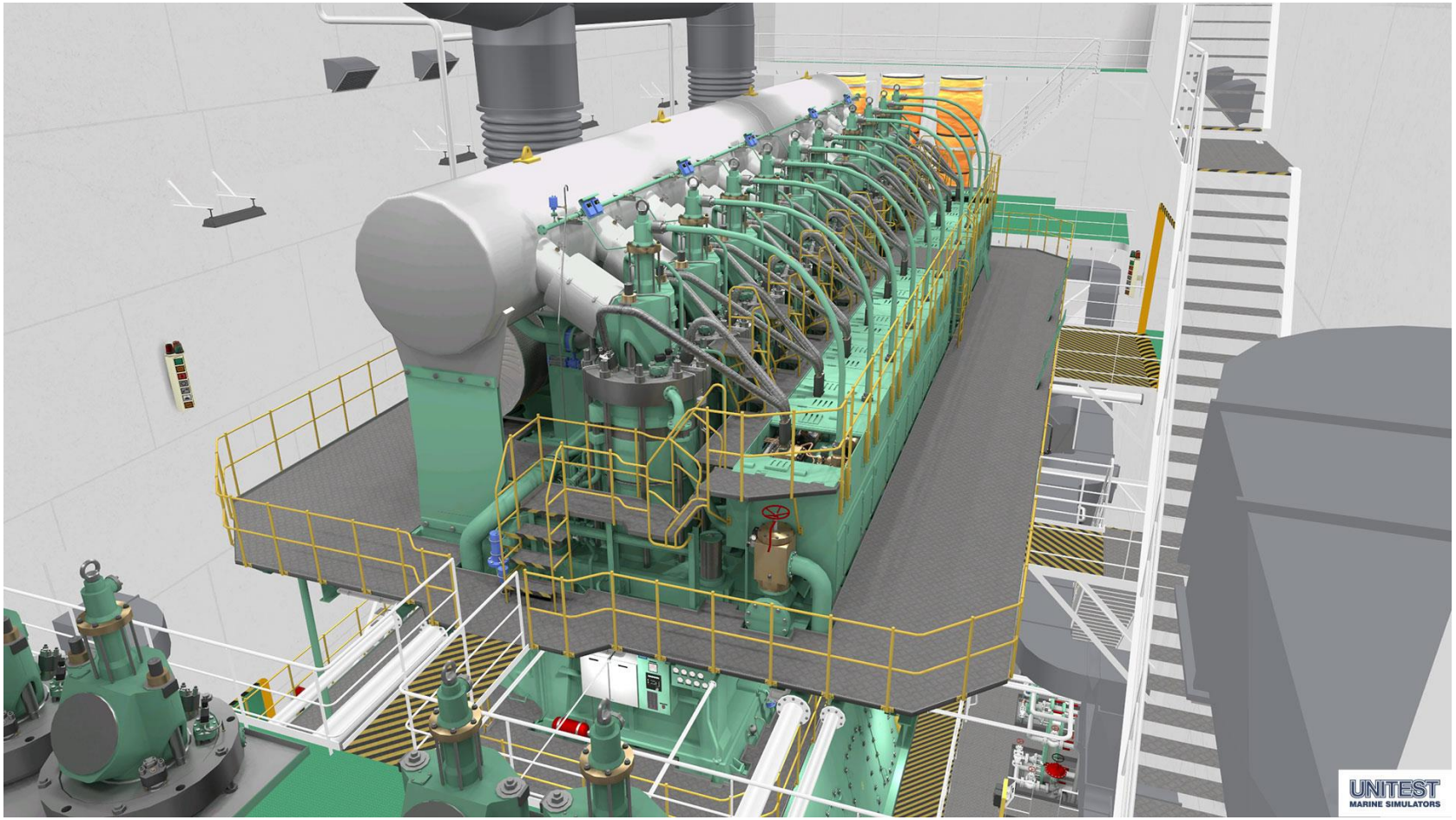
Engine Control Room



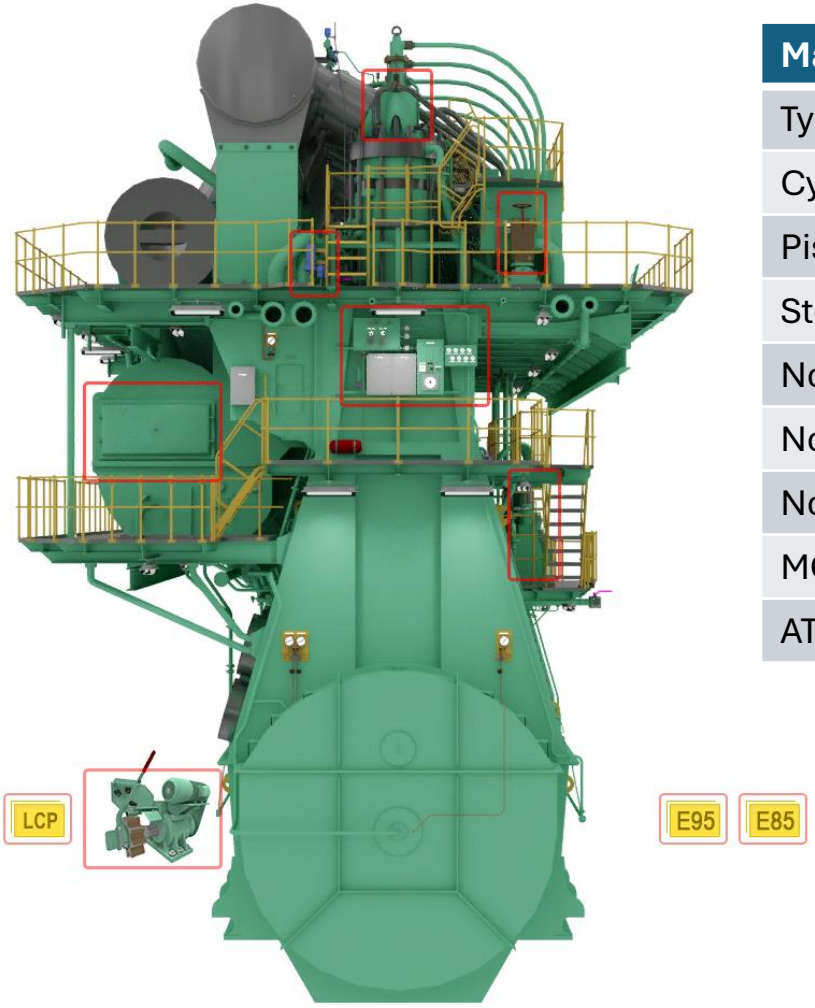
Main Engine Control Diagram



Main Engine – Top View



Main Engine - Side View

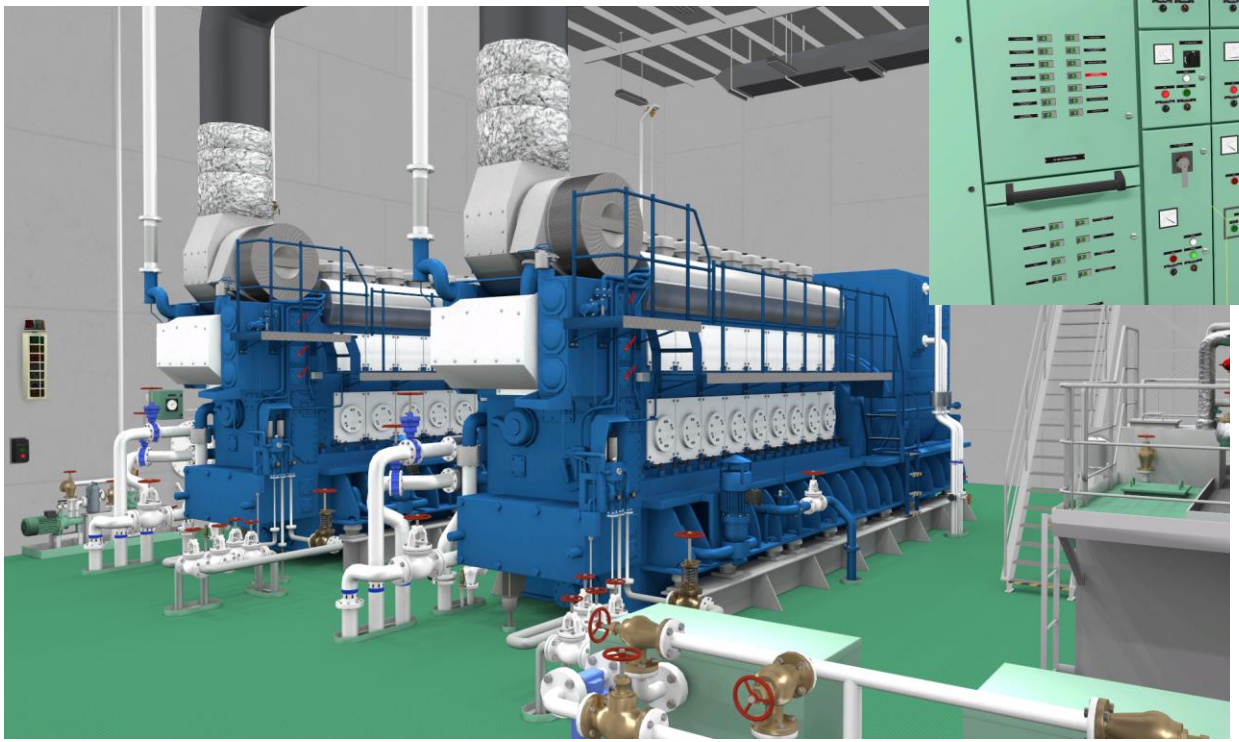


Main Engine Data	Characteristics
Type	Winterthur G&D 10X92
Cylinder Bore	366 m
Piston Stroke	49 m
Stoke / Bore	22kn
No. of Cylinders	148,992 t
No. of Air Coolers	140,872 t
No. of Turbochargers	14,400
MCR	50,190 kW
AT	77.6 RPM

Subsystem Example - Generator

Distribution Panel



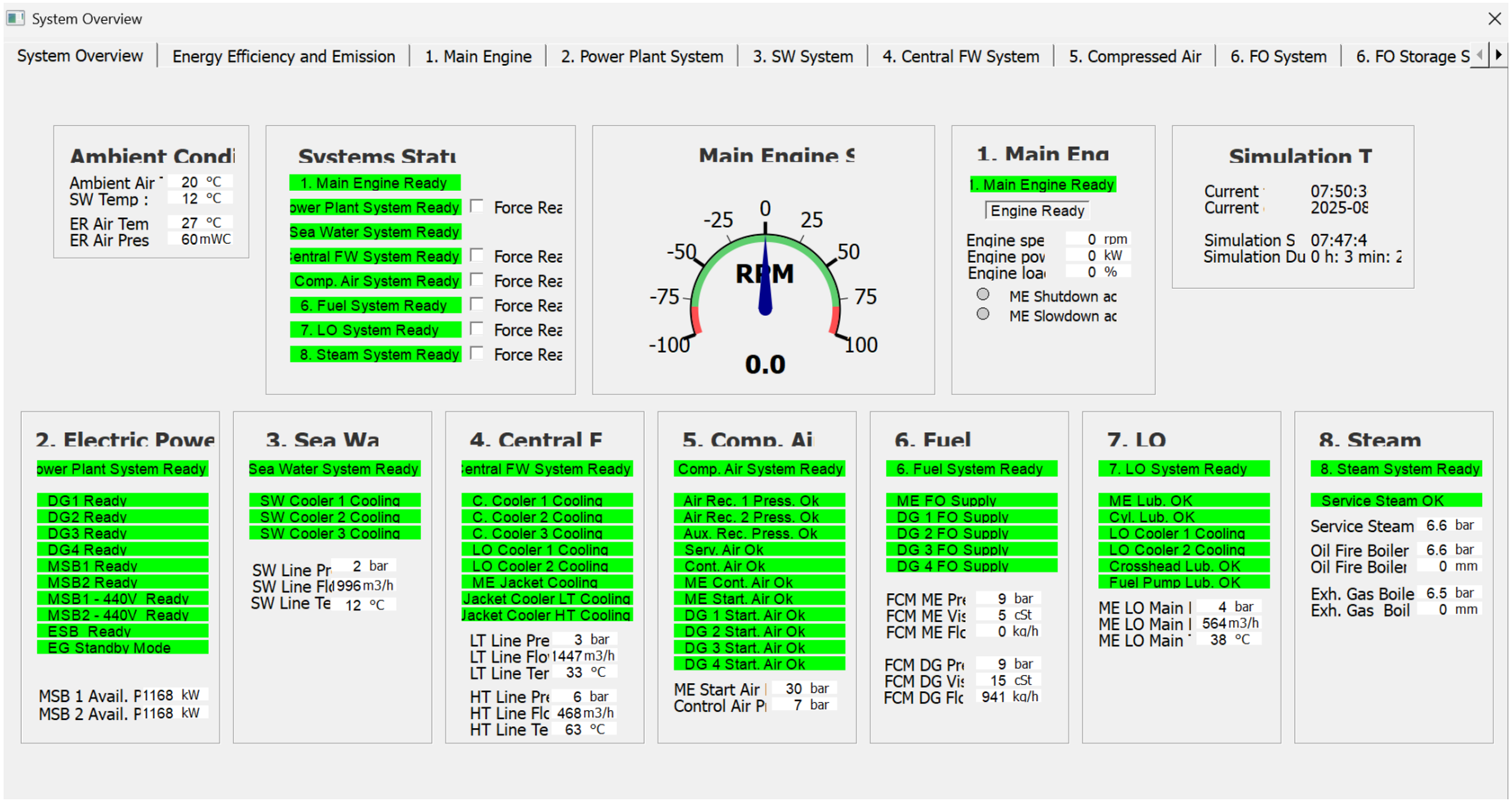




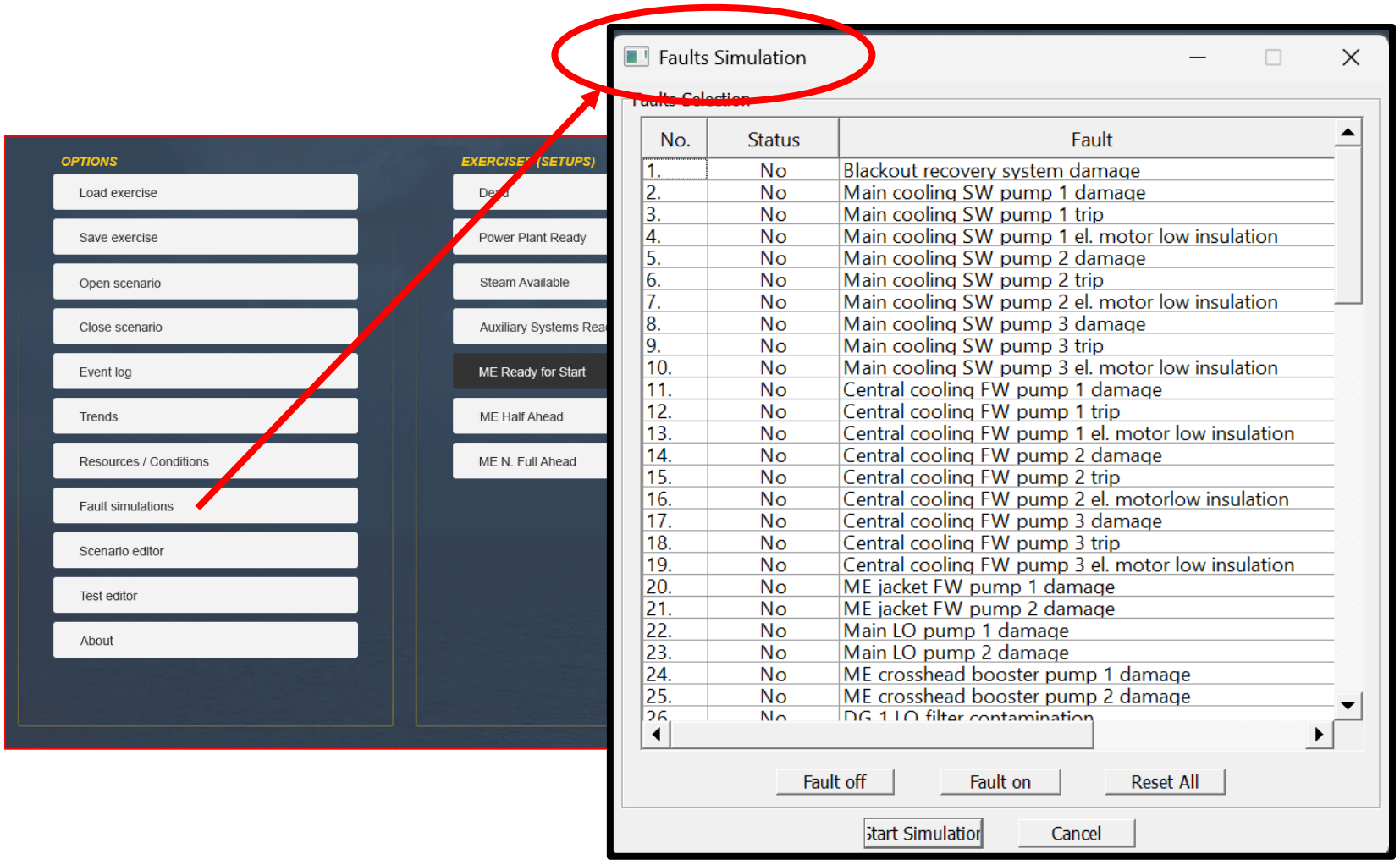
Generator Set – 5 Total

Operator Interface

Operational Status Dashboard



Training Scenarios & Assessment



Preliminary Study Results

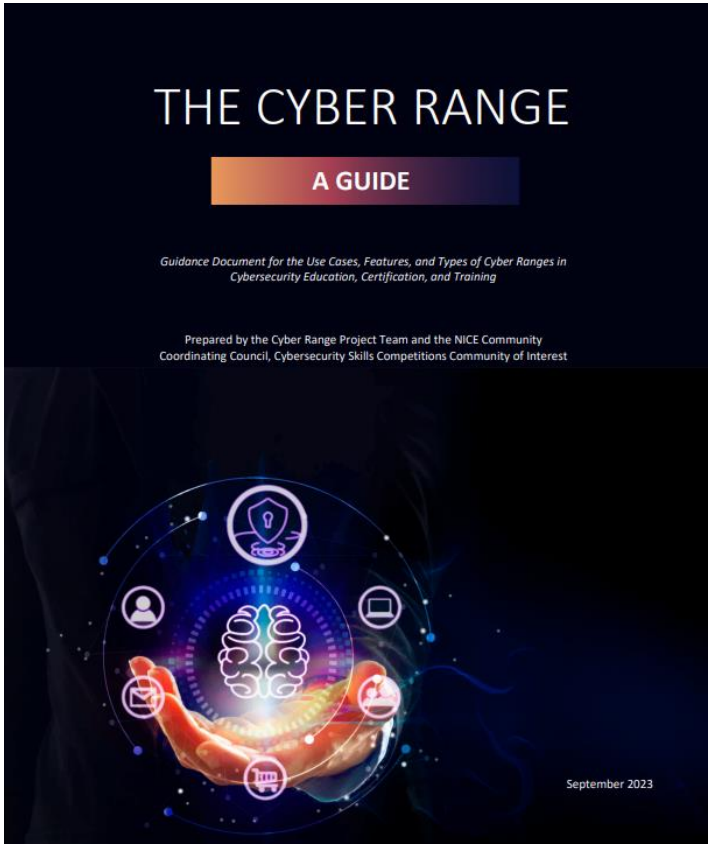
Functional Gaps and Opportunities

Preliminary Simulator Observations

		Gap Impact		
#	Gap - Improvement Opportunities	UC1	UC2	UC3
1	A full ship simulator covering all systems above and below the waterline would be idea. Bridge instrument, and communications gap areas noted. Also, digital infrastructure for hosting ship IT services too.	X	X	X
2	Control diagrams are useful, but a diagram showing discrete and networked digital devices is needed for cybersecurity use.		X	X
3	The simulator fault library does not include any cyber related incidents			X

Phase 2 Study – Area of Interest

Comparative Benchmark



The Cyber Range: A Guide

- Reference Notion of cyber range types
  - Simulation ranges
  - Overlay ranges
  - Emulation ranges
  - Hybrid ranges
- Explore augmenting X92 simulator capabilities
- Linking Unitest's X92 simulator with other relevant synthetic environments like a bridge simulator
- Alternatively integrating Unitest's X92 simulator, a synthetic ship environment, with the physical world which might include testbeds, network simulators, industrial controllers, physical security control systems, etc.



Planned Phase 2 Study Completion Spring 2026

Questions and Constructive Feedback are Always Appreciated!!!

You can find us roaming / working in the MHV.

Alternatively email greerj@uncw.edu

Appendix

A. Acronyms
B. Method Development In Support of Use Case 2

Appendix A - Acronyms

- FMCO – Fleet Management Company
- iBox – Imaginary Box Methods
  - Modeling method developed at UNCW for security domain boundary – attack surface analysis
- MBS2E – Model-based System of Systems Engineering
- SCRM – Senior Cyber Risk Manager
- SOI – System of Interest
- SoS – System of Systems
  - Notion of an Apex System – the system
  - Comprised of Subsystems and Components
- UC – Use Case

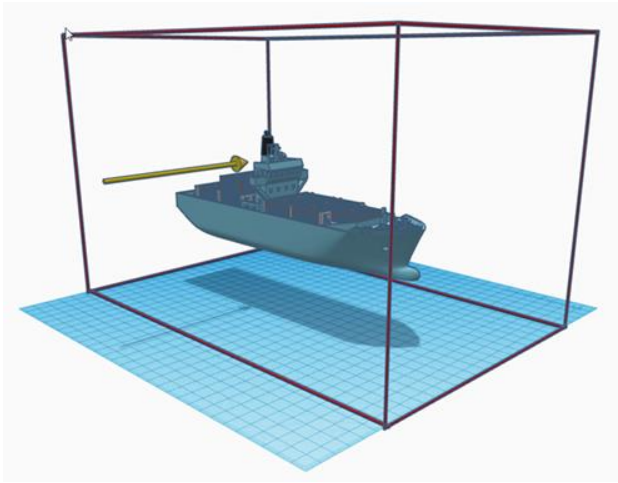
Appendix B - MBS2E

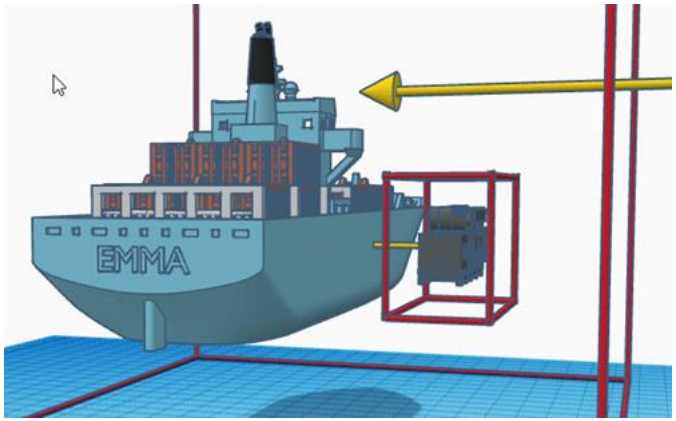
Method Development In Support of Use Case 2

Model-based SoS Cybersecurity Engineering Methods

1. Security Domain Boundary – Attack Surface Analysis
2. Organization Function (Time Based) Attack Surface Analysis
3. System Operational Dependency Analysis
4. Criticality Analysis for Systems and Components
5. Cyber Hazard-Loss Analysis
6. Cyber Risk Management Strategy Design

Security Domain Boundary – Attack Surface Modeling

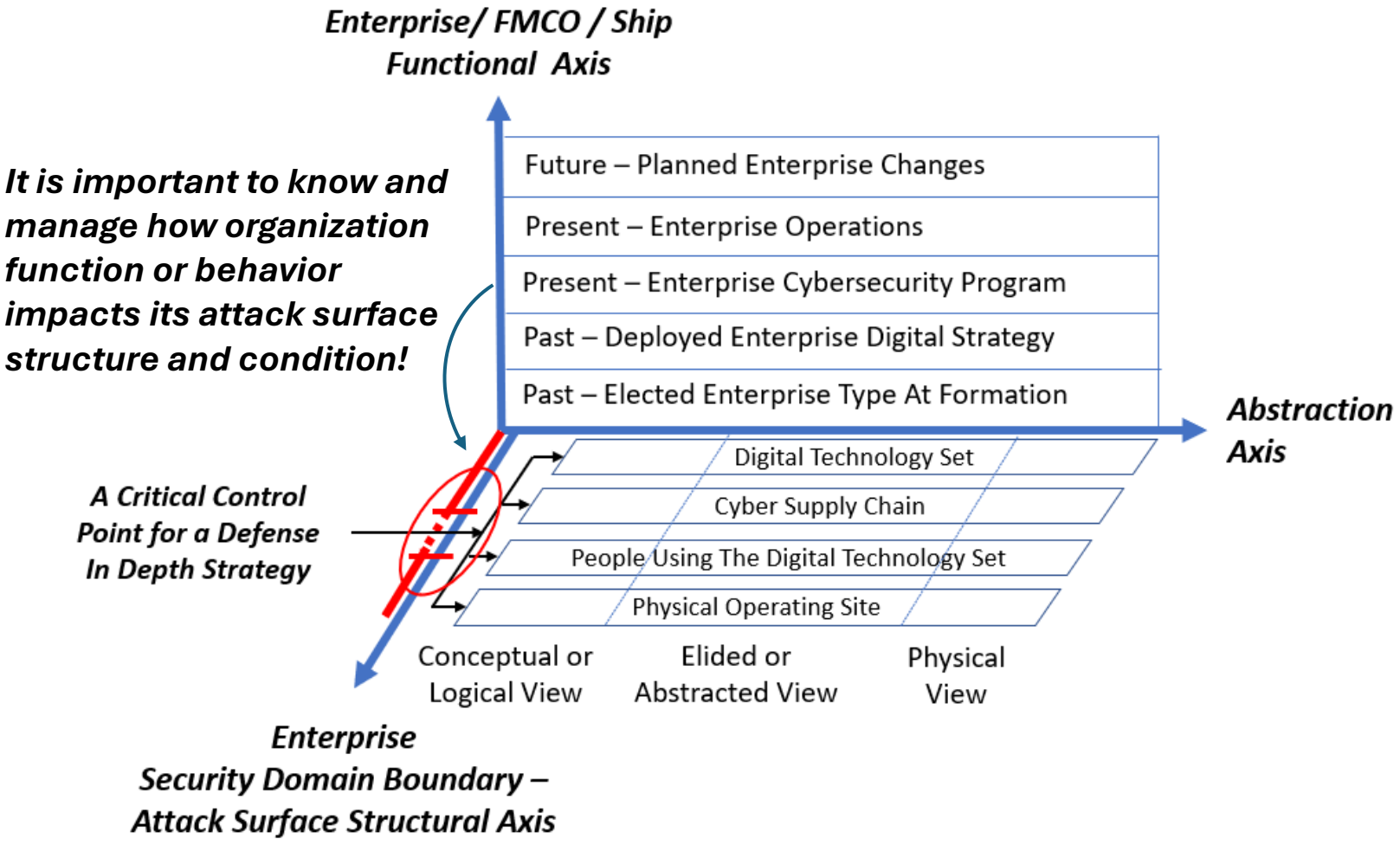




iBox Method

- Place imaginary box around SOI to declare a security domain
- Any force breaking the plane of the box needs to be evaluated as a cyber risk
- 4 Attack surface types
  - Digital
  - Cyber supply chain
  - Authorized employees
  - Unauthorized people attempting to physically breach the security domain boundary

Organization Function Analysis



System Operational Dependency Analysis

NIST 2.0 Identify function … strong on know your digital assets, weaker on knowing the relationships between your digital assets.

Known Coupling Mechanisms

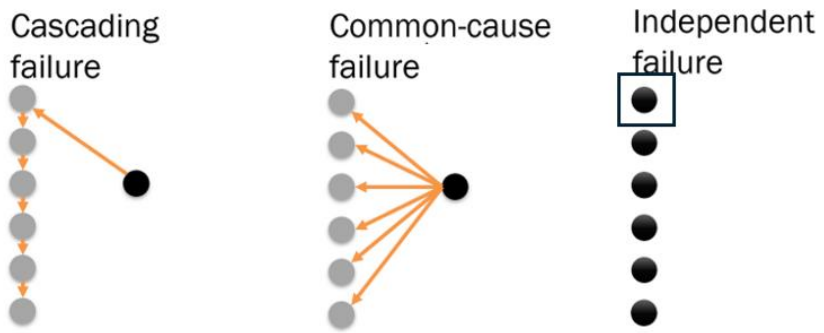
- Mechanical
- Electrical Power
- Communications Network
- Software Applications

Coupled System Decision Making - Control

- Centralized
- Decentralized
- Distributed

Importance of Dependency Analysis

- Need to know converged operating environments containing multiple digital technology types
  - IT / OT / IoT
- Need to know how systems fail



- Application of coupling - dependency knowledge
  - Cybersecurity engineering
  - Safety engineering
  - Resiliency engineering

System Criticality Analysis (CA)

Assess and rank systems by criticality but you first must determine what qualifies as critical.

- Regulatory Requirement
- Safety Requirement
- Security Requirement
- Resiliency Requirement
- Mission Requirement
- Organization Function Requirement
- Other TBD

Cyber Hazard-Loss Analysis

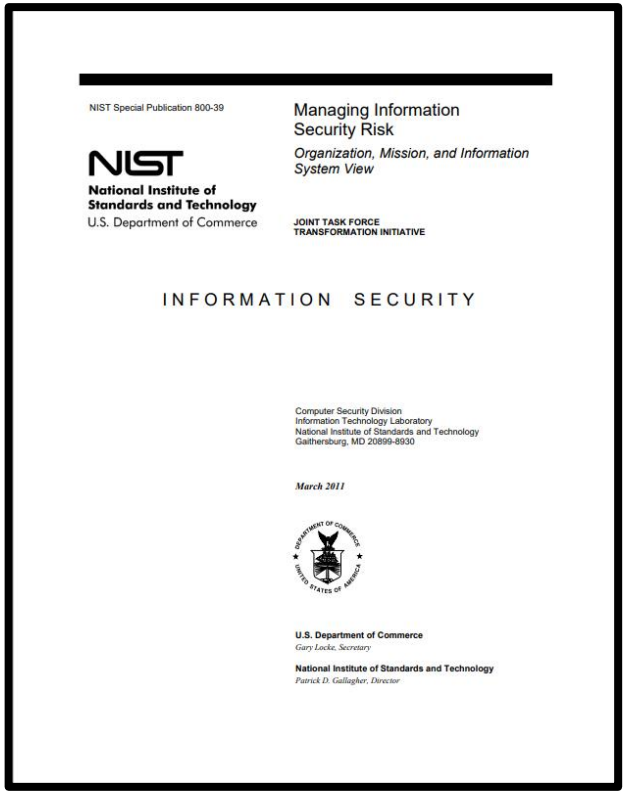
Information Sources for Informed Decision Making

- Known Insurance Loss Payouts
  - International Union of Marine Insurance
  - Major claims database
  - Major Claims Database 2024 | IUMI
  - et.al
- Threat Intelligence
  - MTS-ISAC
  - USCG
  - CISA
  - et.al.

Analysis Methods

- MIT
  - System Theoretic Process Analysis for Security (STPA-Sec)
  - STPA-Sec-Tutorial.pdf
- MITRE
  - Threat Assessment and Remediation Analysis (TARA)
  - Threat Assessment and Remediation Analysis (TARA) | MITRE

Cyber Risk Mgmt. Strategy Design



NIST Special Publication 800-39

Managing Information Security Risk

Organization, Mission, and Information System View

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

NIST SP800-39

