A Transdisciplinary Approach to Maritime Transportation System Cybersecurity Education and Capability Development

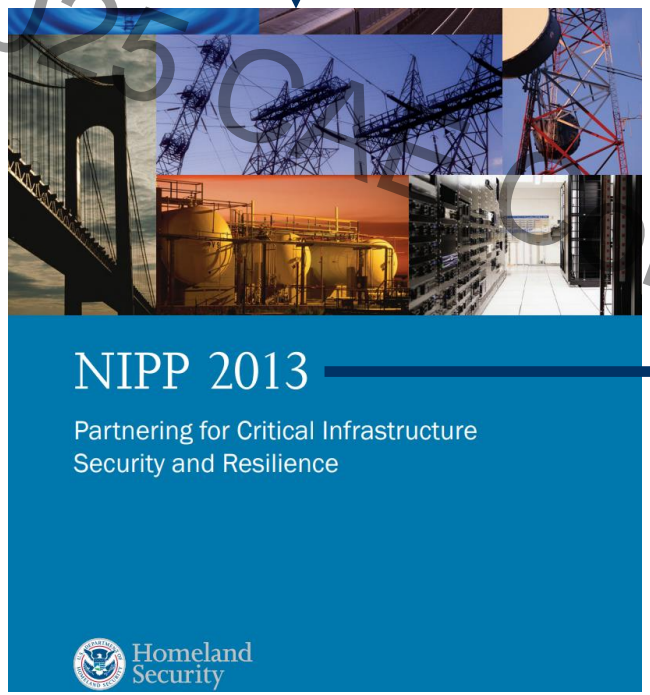
Presented to NSA-CAE Conference

by Jeff Greer | Lecturer, Cybersecurity | @ UNCW
On Behalf of The Authors

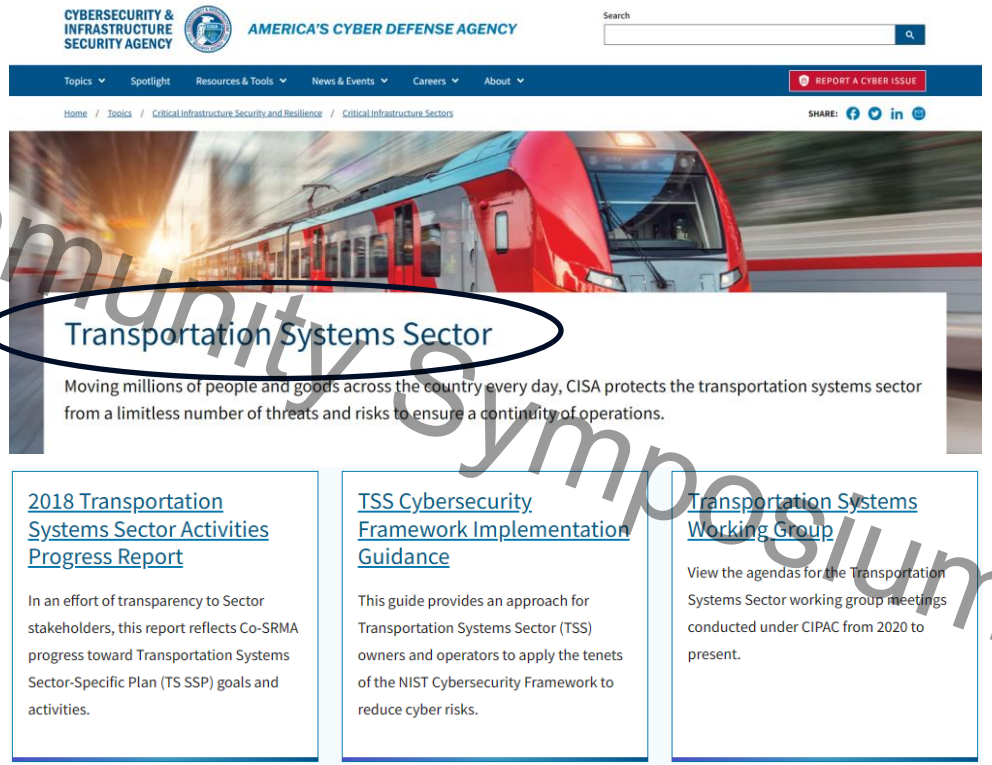
CCDE
UNCW Center for Cyber Defense Education

Background

Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience



16 Sectors Identified



CCDE
UNCW Center for Cyber Defense Education

Motivation – Two Questions That Merit Consideration

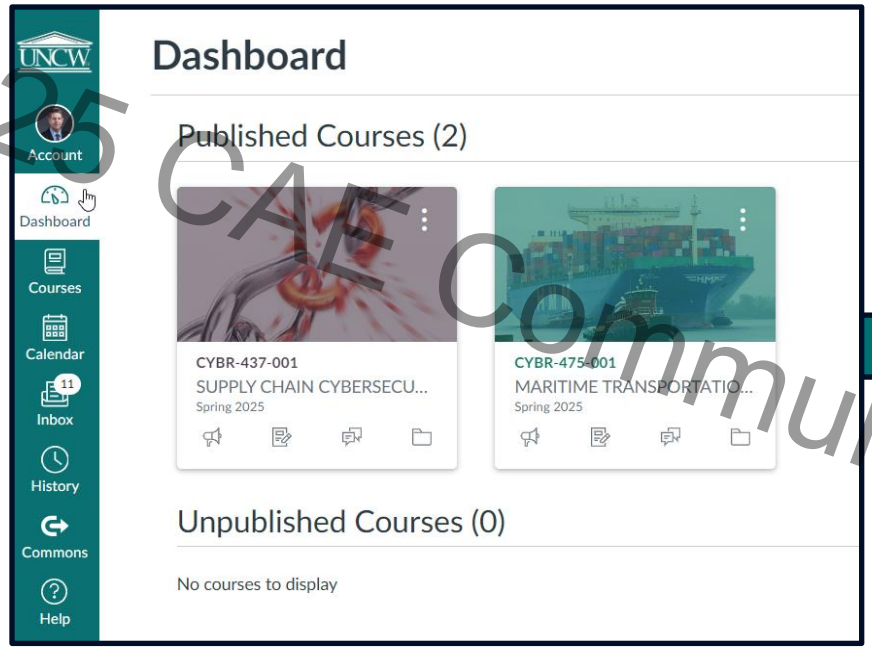
- What is the optimal applied cybersecurity training program for maritime and other critical infrastructure operators?
- What improvements can be made to accelerate student KSA development and advancement into leadership positions?

Teach Critical Thinking Skills

Reality – Technologies Come and Go over a Career …
Critical Thinking Skills Are Forever and Enable Effectiveness

5 Key Questions Students Need to Ask & Learn How to Answer	For a Named System of Interest (SOI)
1. What is it?	Ship (Stereotypical or named)
2. Why does it matter?	<Security Scope Determination>
3. How does it work	<Functional Modeling>
4. How can it fail	<Hazard Loss Analysis>
5. How can failure be managed?	<Strategic and Tactical Cyber Risk Management Strategy Design>

Canvas – UNCW's Learning Management System



Virtual Ship Training Environment

Jeff Greer
Kasey Miller

Physical Test Bench Training Environment

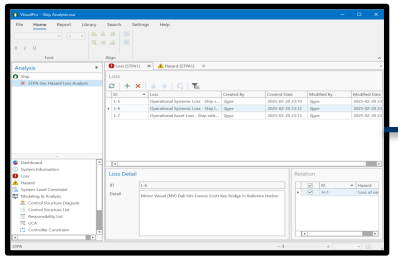
Hosam Alamleh
And Bilge Karabacak

Ulku Clark and Geoff Stoker
Program Development

CCDE
UNCW Center for Cyber Defense Education

Virtual Ship Training Environment Overview

OSINT Consequence-Driven Hazard Loss Analysis



WVAY – STPA-Sec With STRIDE

OSINT Cyber-Informed Threat Intelligence

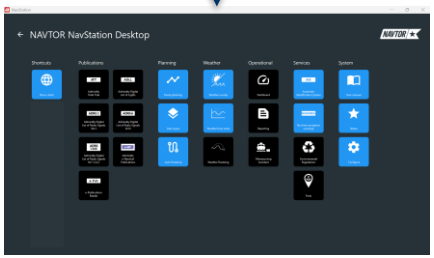
MCAD Cyber-Attack DB

Creative Guidance:

The DoD Cyber Tabletop Guide
NICE, The Cyber Range, A Guide
The 5 W's of Systemigrams

UNCW Maritime LMS Library

Address Targeted Educational Needs



NAVTOR
Navigation Planning

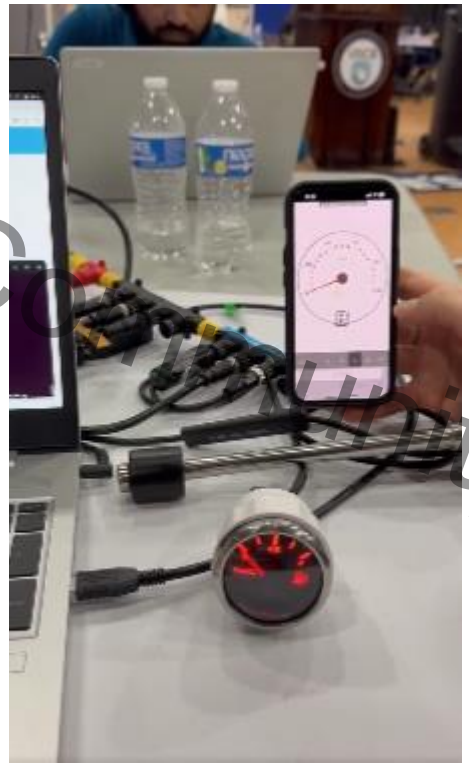
Nautis (Cloud)
Bridge Simulator

Dr. Kluj @ Unitest
Engine Simulator

INL M-DAT
Incident Management

CCDE
UNCW Center for Cyber Defense Education

Test Bench Training Environment



CCDE
UNCW Center for Cyber Defense Education

UNCW Maritime LMS Library Content

Educational

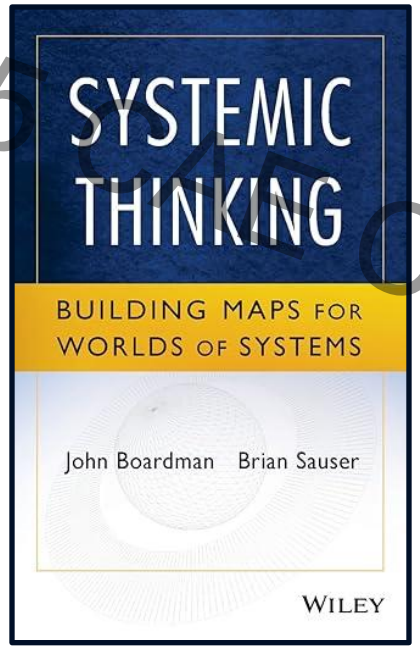
- Learning Objectives
- Lesson Plans
- Lab Plans
- Tabletop Exercises
- Assessment

Reference Materials

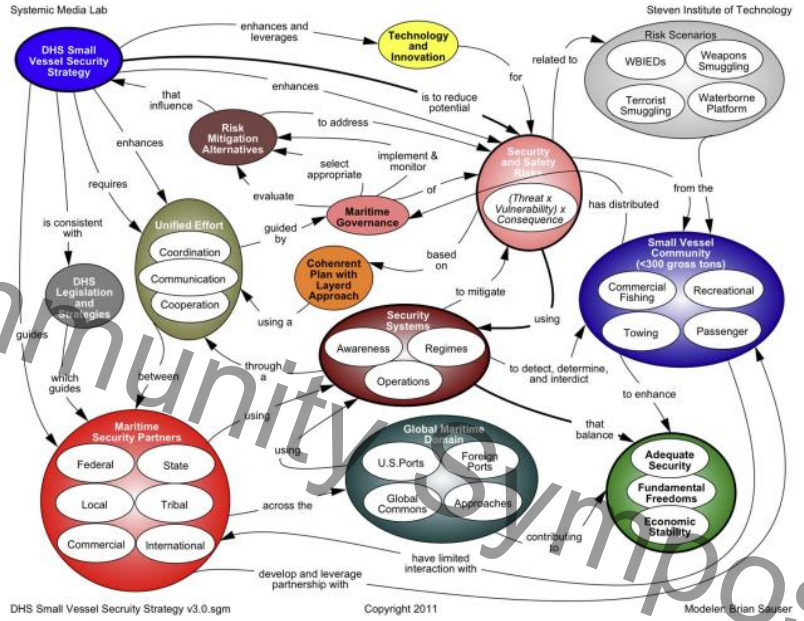
- Relevant OSINT Sources
  - Industry Awareness
  - Maritime Losses
  - Threat Intelligence
- Safety Regulations
- Technical Standards
- Free Online Training Resources

Note: It is the library that integrates all the single function simulators, specialized software programs, and content for education delivery!

Teach System Thinking Skills



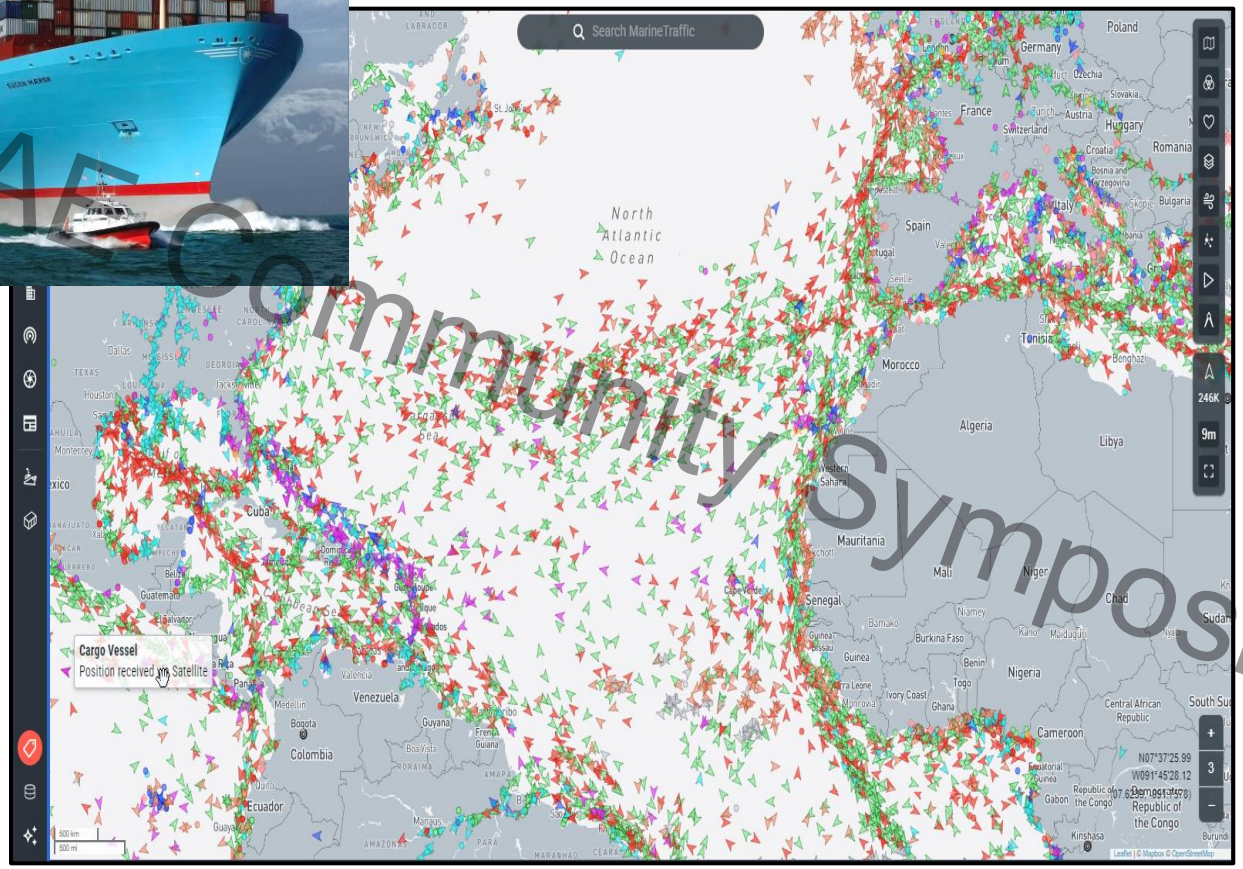
Design Tools



Source: Systemigram Modeling of the Small Vessel Security Strategy for Developing Enterprise Resilience

CCDE
UNCW Center for Cyber Defense Education

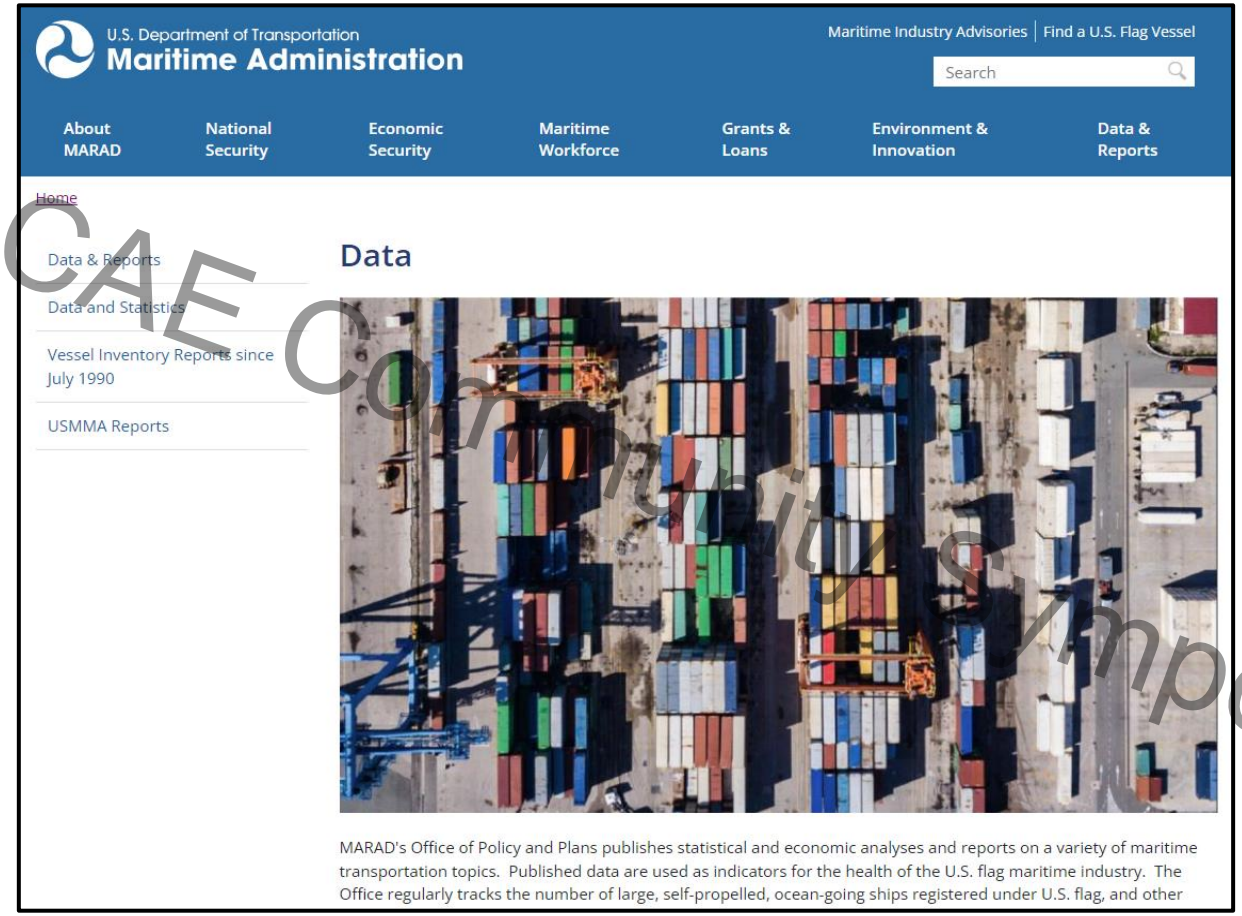
Maritime Industry Knowledge



MarineTraffic.com

CCDE
UNCW Center for Cyber Defense Education

Maritime Commercial Knowledge

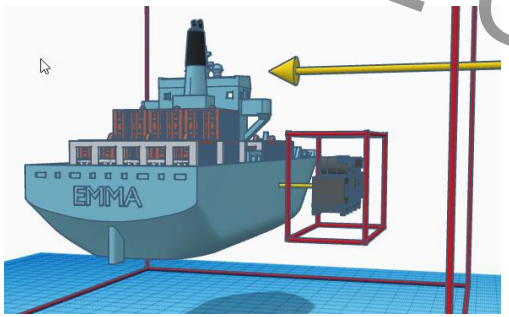


DOT (MARAD) Shipping Statistics

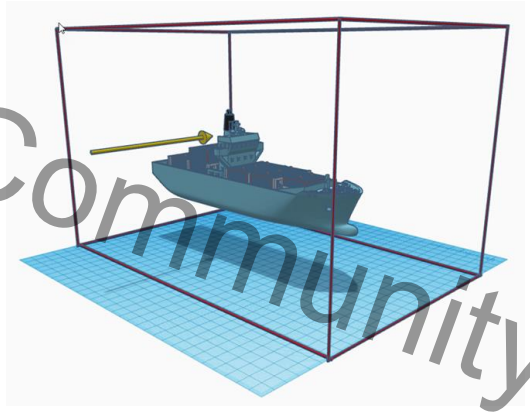
CCDE
UNCW Center for Cyber Defense Education

Teach System Engineering Skills

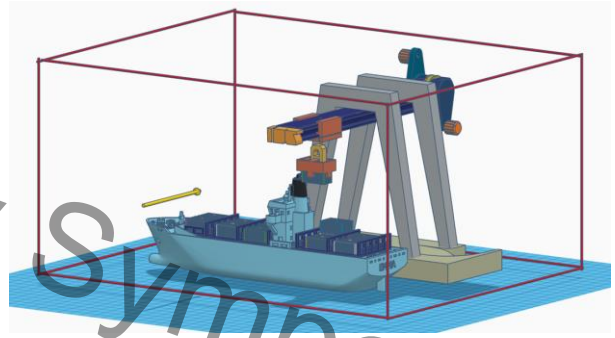
Security Domain Boundary Modeling – iBox Method Developed @ UNCW



Sub-Domain – Engine Room



SOI Security Domain Boundary



Super Domain – Ship + Port

Models Developed in TinkerCad
With Thinglverse.com 3D Models

CCDE
UNCW Center for Cyber Defense Education

Source John Boardman and Edward Bowers

Manage the Convergence of Multiple Critical Systems Within a Single System of Interest Security Domain

Critical System Types	Utilized Digital Technologies	Security Objectives
Informational	IT	CIA
Operational	OT, IoT, CPS	Safety
Military	Sensors and Kinetic Weapons	Mission Achievement

CCDE

UNCW Center for Cyber Defense Education

Network Segmentation and Integration Point Management Design

Maritime Domain Specific Technical Knowledge

Abstracted Functional Ship Control Model

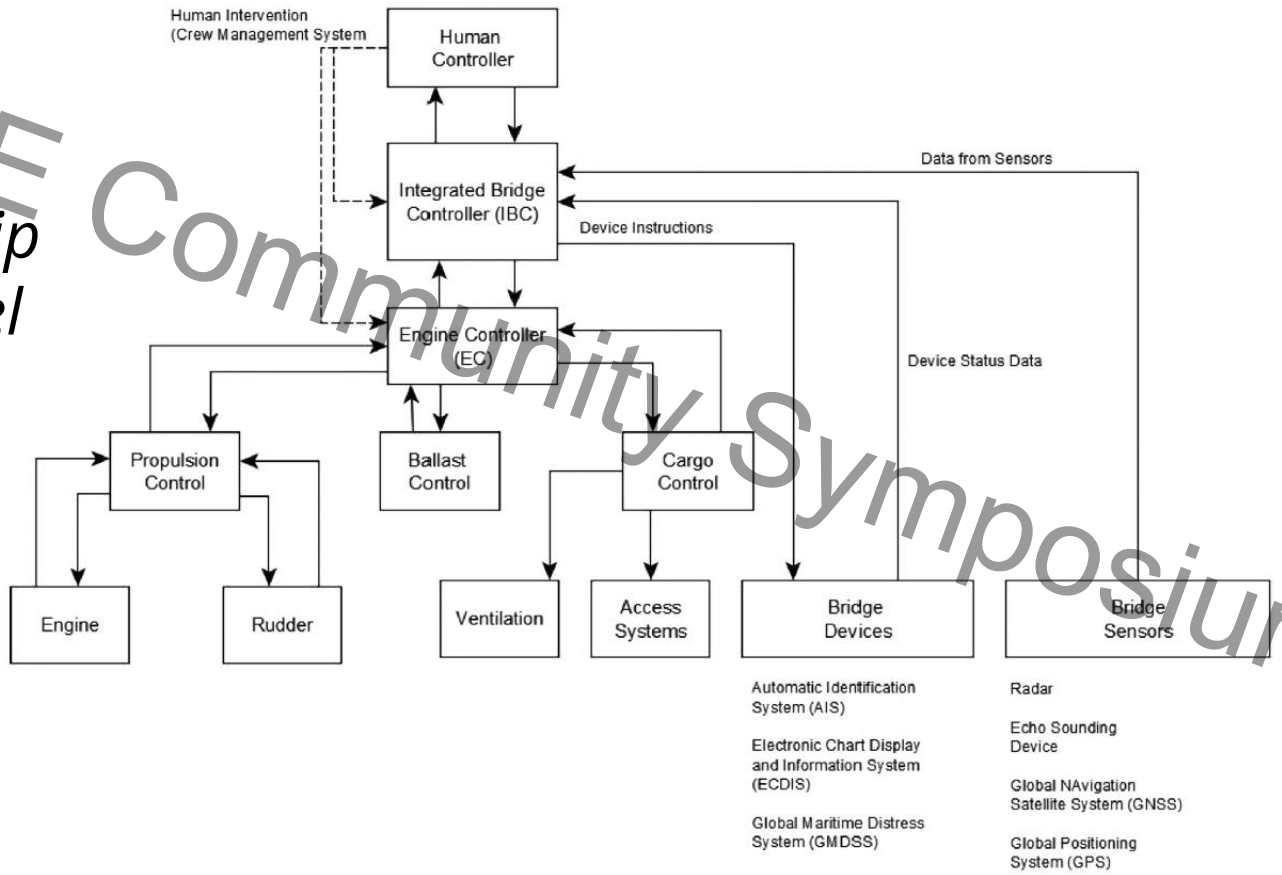
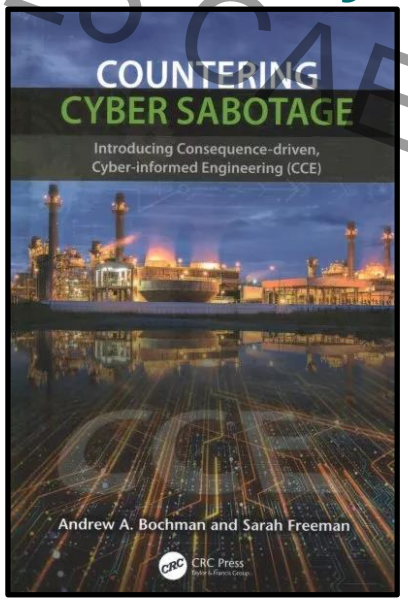


Fig. 1. CyberShip framework.

CCDE
UNCW Center for Cyber Defense Education

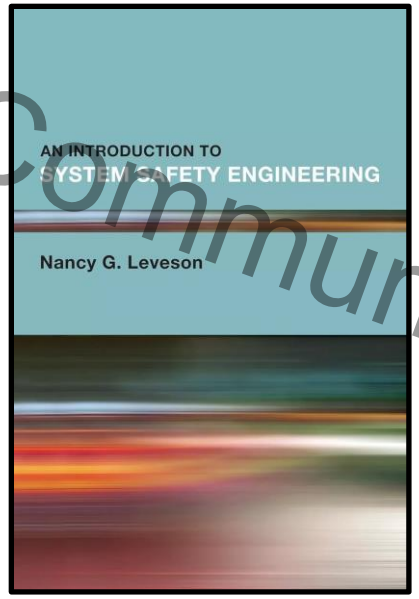
Teach Safety Engineering Skills

INL Theory



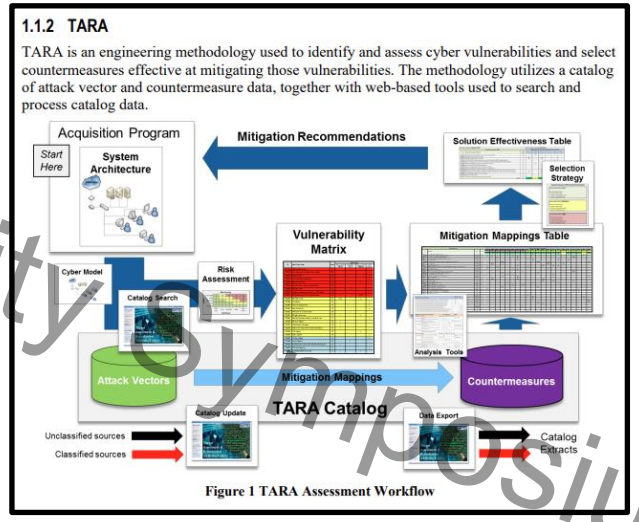
INL CCE Website

MIT Theory



MIT PSASS Website

MITRE Theory



MITRE TARA Website

CCDE
UNCW Center for Cyber Defense Education

Why Safety Matters

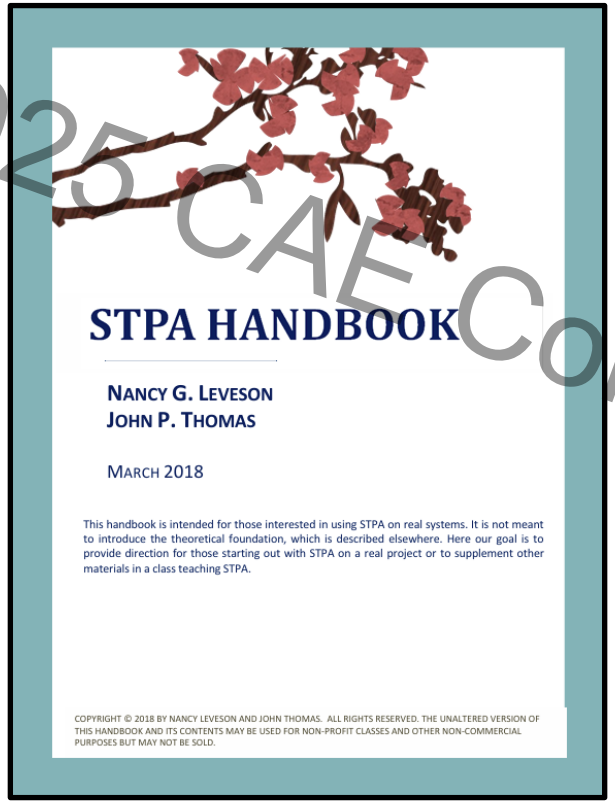
- Design goal – a secure digital operating environment free from fault
- Alternatively, one that fails safe and recovers quickly

Start Here → Work Left to Right →

Direct and Consequential Losses to Avoid	ID Hazards Triggered by a Cyber-Attack	Conduct a Hazard Risk Analysis	Select Appropriate Risk Treatments

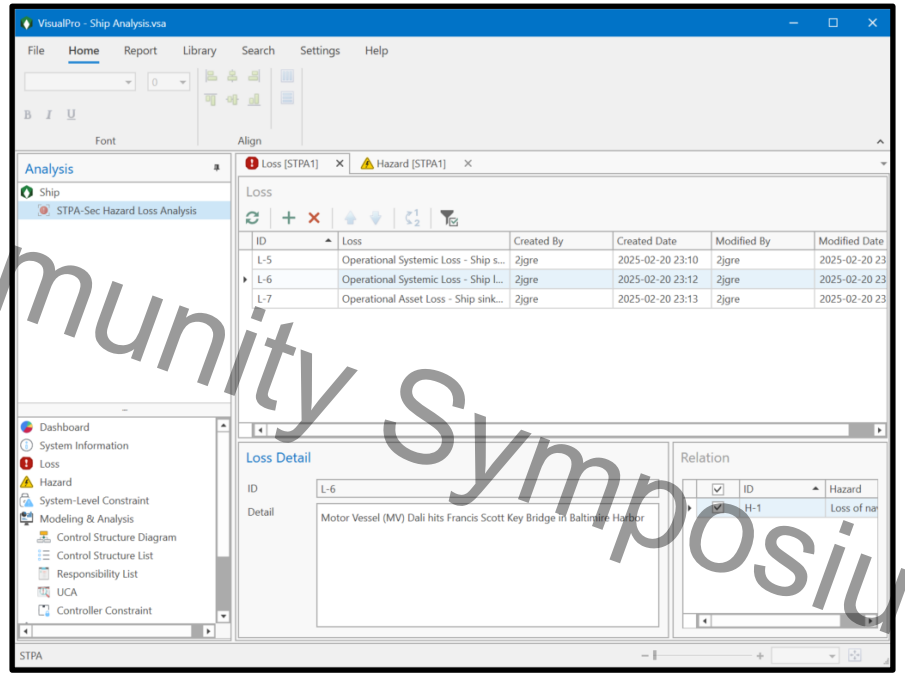
Note: The spectrum of risk treatments now includes classic security controls, dynamic countermeasures, and resilient digital infrastructure design.

Utilize Hazard Loss Analysis Tools



MIT PSASS Website

VWAY - VisualPro



Hazard Loss Analysis Application

CCDE
UNCW Center for Cyber Defense Education

Teach Cybersecurity Engineering Skills

- **SbG – Security by Governance**
  - Design an effective cybersecurity program enabling security goal and objective achievement
- **SbD – Security by Design**
  - Design a secure digital operating environment
- **SbO – Security by Observation**
  - Design a monitoring capability to assure the digital operating environment design is secure
- **SbR – Security by Response**
  - Design a cyber incident response capability to contain and remediate a discovered cyber-attack
- **SbA – Security by Assessment**
  - Design an assessment methodology for adaptive learning and continuous improvement over time

Near Term – Tool Enable Next Gen Cyber Defenders to Counter Adversarial AI

Novel Engineering Workstation Design

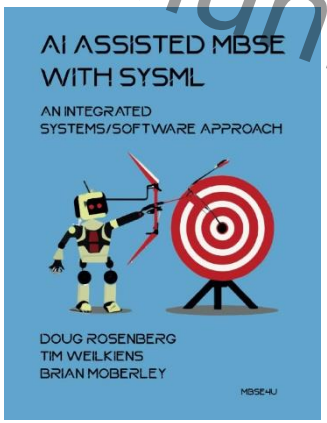
Improve Decision Making Speed and Effectiveness!

Proof of Concept in Development @ UNCW

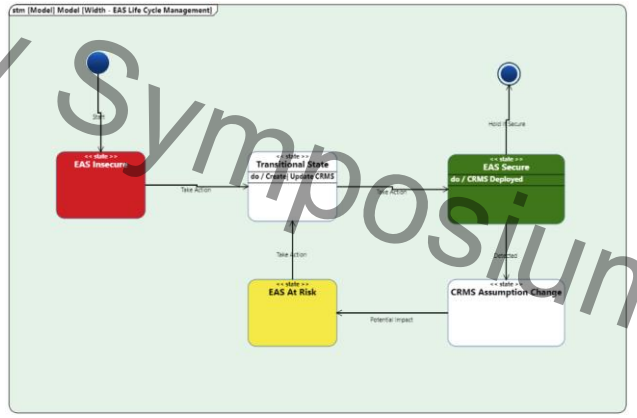
for Student - Senior Cyber Risk Manager Use

Enterprise Attack Surface Model

Digital Twin - Persistent Real Time Data Fabric For Design Use



Cyber Risk Mgmt. Strategy Design and Deployment



State Machine Approach for Managing the Enterprise Attack Surface

CCDE

UNCW Center for Cyber Defense Education

Questions and Comments

Constructive Feedback Is Appreciated!

Contact: greerj@uncw.edu

CCDE
UNCW Center for Cyber Defense Education