Cyber Resiliency in Naval Engineering Systems

GOAL: Maintain the operability of U.S. Coast Guard ships during cyber attacks

Ryan Montvydas & Dr. Keri Pearlson

1. Cyber Resiliency is a Key Component of Cybersecurity

Cyber resilience acknowledges that risk can not be mitigated to reduce vulnerabilities to 0 and therefore needed to maintain the ability to perform

Risk Mitigation + Resiliency = System Performance

Therefore…

Cyber security + cyber resiliency = Cyber-Physical System Performance

Equation 1:

2. Hypothesis: Cyber Resiliency Will Reduce Ship Downtime

Naval System Cyber Resiliency: Maximizing a ship's engineering system performance during a cyber incident to ensure the minimum operating level of a vessel is maintained.

Hypothesis: Cyber resilience can be identified for Naval Engineering Systems as a parallel to cyber security to reduce potential physical system downtime caused by a cyber incident.

"Information System Resilience: The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack." (NIST pub.800-30)

For more information:
contact: Ryan Montvydas rmonty@mit.edu

3. Steps to Resolve Cyber Resiliency Gaps

1) Discuss system needs with stakeholders
2) Define cybersecurity vs. cyber resiliency
3) Conduct System Theoretic Process Analysis (STPA)
    1) Define system
    2) Model control structure (Fig. 1)
    3) Identify cyber-resiliency gaps
    4) Create cyber-resiliency requirements
4) Generate scenario-based recommendations

4. Apply a Holistic System Model to Test Cyber Resiliency

Through modeling a system's control structure, cyber-resiliency gaps can be identified. Necessary cyber-resilience requirements based on the control structure can then be created. See Figure 1 for control structure

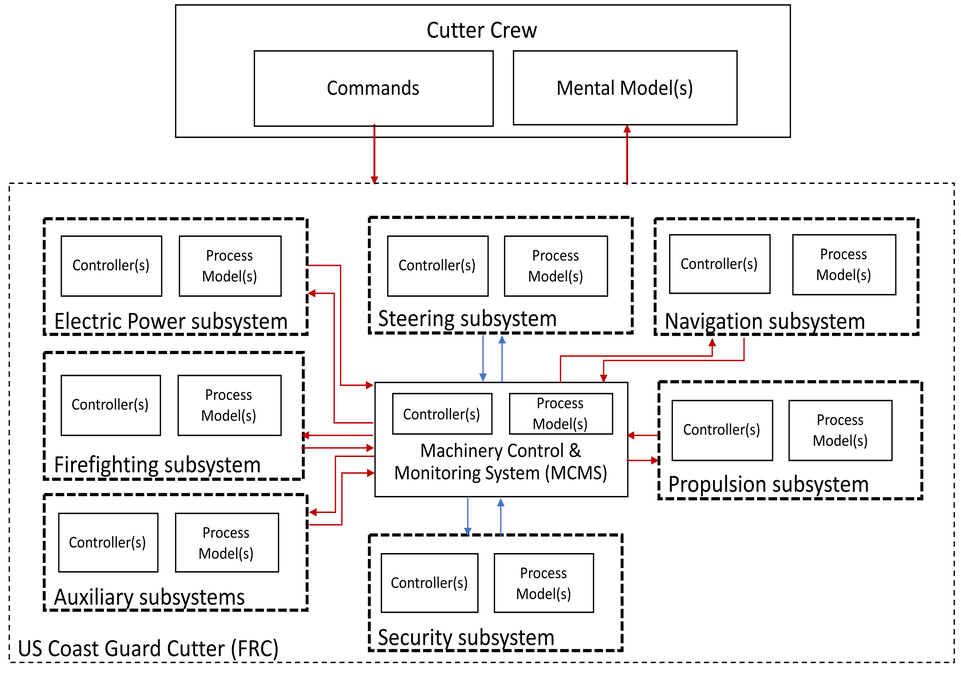

Figure 1: System Boundaries (dashed lines) & Interactions (Red line indicates control & feedback; Blue line indicates information transmission)

5. Lessons for Implementing Cyber Resiliency Practices with Cybersecurity

1) Cybersecurity & cyber resiliency are crucial to a system's 'uptime'; it's not an either-or choice.
    1.1) Cyber resiliency is tested when a cyber-attack occurs. Cybersecurity is tested when cyber-attacks don't occur.
2) Managers should select and prioritize key functions that must have cyber-resiliency for their system to deliver its intended value. Then create testable scenarios of detection, response, and recovery.
3) Resilience is not enough to respond to a cyber attack. Cyber attacks could disrupt multiple systems simultaneously and degrade organizational performance. Cyber resilience is required of all socio-technical systems within an organization.