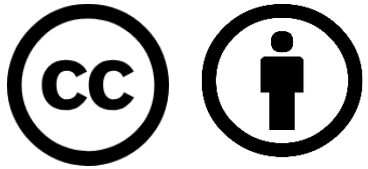
Cybersecurity

Shipboard Power System Fundamentals

Revision of 6 February 2026

Dr. Norbert Doerry



Essential Questions

What risk management processes for addressing shipboard machinery control cybersecurity are used?	Understand
How can cybersecurity be implemented in a shipboard power system?	Understand
How can cybersecurity implementations impact the operation of a shipboard power system?	Understand

Cybersecurity - threats

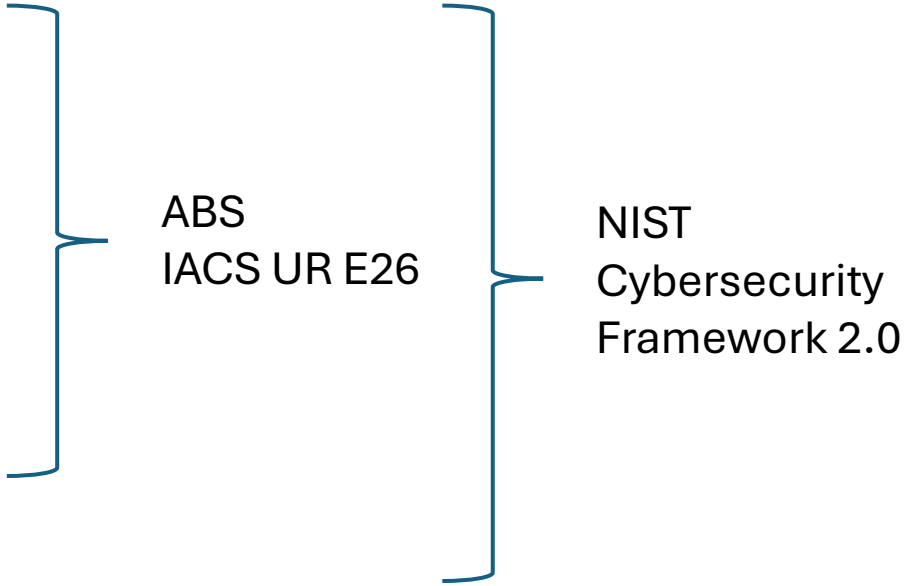
- Onboard ship
  - Introduced during manufacturing at OEM
  - Prior to installation onboard ship
  - Malicious actors onboard ship
    - Ship’s crews
    - Maintenance personnel
    - Visitors
    - Other
  - Inadvertent actors – usually careless members of ship’s crew.
- Off the ship
  - Cyberattacks

Cybersecurity risk management

- Risk Management
  - Identify possible negative outcomes
  - Tracing possible negative outcomes to causes
  - Assessing the likelihood and impact of the possible negative outcomes
  - Assigning a level of risk to the possible negative outcomes
  - If level of risk is assessed high enough, develop and implement risk mitigation plans
- Cybersecurity Resilience
  - Framework for implementing cybersecurity risk management
  - Procurement of applicable onboard systems and equipment should include requirements for cybersecurity resilience

Elements of cybersecurity resilience

- Identify
- Protect
- Detect
- Respond
- Recover
- Govern



Identify

- Configuration management of computer-based systems
  - Regularly inventory hardware and software
  - Ensure other elements are applied to all computer-based systems
- Periodic review of documentation describing roles and responsibilities of personnel in the management, operation, and governance of computer-based systems
  - Ensure documentation is up to date and configuration managed
  - Ensure personnel are aware of their roles and responsibilities

Protect

- Implement safeguards to limit or contain the impact of a cybersecurity incident
- Group computer-based systems into security zones
  - Stand-alone or connected to other security zones or networks through controlled data communication
  - Security zones should align with ship's zone boundaries where possible
  - Controlled data communication implemented via …
    - Firewalls
    - Routers
    - One-way data flow techniques
- Avoid or mitigate the impact of denial-of-service (DoS) attacks
- Employ antivirus, anti-malware, and antispam software
- Use access controls (user and device authentication)

Detect

- Implement methods to recognize and identify inappropriate activity within a computer-based system
- Verify that the computer-based system correctly implements security functions

Respond

- Minimize the impact of a cyber event on a computer-based system and associated networks
- Prevent the cyber event from impacting other computer-based systems
- Develop and configuration manage incident response plans
  - Train personnel to respond to cyber events using the incident response plans
- Techniques
  - Redundant computer-based systems
  - Local controls that serve as backup to primary control system (required for some computer-based systems by IMO)
  - Stop network communication into or out of a security zone (computer-based systems within the zone should still be capable of functioning)
  - Should be capable of putting a computer-based system into a safe state

Incident Response Plan contents (IACS UR E26)

- Breakpoints for the isolation of compromised systems
- Description of alarms and indicators signaling detected ongoing cyber events or abnormal symptoms caused by cyber events
- Description of expected major consequences related to cyber incidents
- Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control
- Independent and local control information for operating independently from the system that failed due to the cyber incident

Recover

- If possible, restore all computer-based systems and associated networks to normal operation
- Develop and configuration manage recovery plans
  - Train personnel to respond to cyber events using the recovery plans
  - Base recovery plans on recovery objectives (IACS UR E26)
    - System recovery: methods and procedures to recover communication capabilities shall be specified in terms of Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.
    - Data recovery: Recovery Point Objectives (RPO) should specify methods and procedures to recover data necessary to restore safe state of the hardware, software and networks that monitor and control onboard systems and to restore safe ship operation. The longest period of time for which an absence of data can be tolerated should be specified.

Recovery plan contents (IACS UR E26)

- Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.
- Processes and procedures for the backup and secure storage of information.
- Complete and up-to-date logical network diagram.
- The list of personnel responsible for restoring the failed system.
- Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.
- Current configuration information for all components.

Cybersecurity operational impact

- Cybersecurity is not passive
  - Crew training is critical
  - Documentation supporting cybersecurity resilience should be regularly reviewed and updated
  - Regular exercises should be carried out on detecting, responding, and recovering from cyber incidents
- Cybersecurity requires an investment in crew time and resources
  - Payoff is fast recovery in response to a cyber incident
  - Lost operational time can be very expensive