Cybersecurity

Norbert Doerry

December 2, 2025

1. Introduction

Shipboard power systems are increasingly using networked computer-based systems (CBS). These CBSs may be vulnerable to malicious actions from a variety of threats. These threats may be onboard the ship, or may be located off the ship in remote locations. Onboard ship, these threats may have been introduced during the assembly of equipment at the original equipment manufacturer (OEM), prior to installation onboard ship, by malicious actors onboard ship, or inadvertently by members of the ship's crew. The resilience of shipboard systems to these threats is typically achieved through a multi-layer risk management approach. Five elements of cybersecurity resilience as defined by ABS (2025) and IACS UR E26 are:

- Identify
- Protect
- Detect
- Respond
- Recover

The NIST Cybersecurity Framework 2.0 includes these 5 elements and adds another called "Govern."

The laws, regulations, class society rules, standards, and specifications governing cybersecurity are continuously evolving. The reader is advised to consult the latest versions of shipbuilding specifications, governing documentation and references to ensure ship designs are achieving up to date cybersecurity implementations.

2. Cybersecurity risk management

Risk management in general is composed of identifying possible negative outcomes, tracing these outcomes to causes, assessing the likelihood and impact of the possible negative outcomes and assigning a level of risk to the possible negative outcome. If the level of risk is assessed to be high enough, risk mitigation plans are developed and implemented. The implementation of cybersecurity resilience elements is intended to address cybersecurity risk management.

The procurement of applicable onboard systems and equipment should include the requirements for cyber resilience detailed in IACS UR E27.

3. Cybersecurity resilience implementation

The following guidance is from IACS UR E26:

3.1. **Identify.** The identify element incorporates both configuration management of CBSs and an understanding of the roles and responsibilities of personnel in the management, operation, and governance of CBSs. All hardware and software associated with the CBSs should be regularly inventoried (typically annually) to ensure the configuration management is up to date throughout the ship's service life. Similarly, documentation describing the roles and responsibilities of personnel in the management, operation, and governance of CBSs should be configuration managed and regularly reviewed (typically annually) to determine if the documentation should be updated.

3.2. **Protect**. The protect element seeks to implement safeguards to limit or contain the impact of a cybersecurity incident. CBSs are grouped into security zones which are either stand-alone, or connected to other security zones or networks through controlled data communications. Where possible, security zone boundaries should align with the ship's zone boundaries. Controlled data communication is typically implemented via firewalls, routers, and one-way data flow techniques. Protect also includes techniques to avoid or mitigate the impact of denial-of-service (DoS) attacks; the employment of antivirus / antimalware / antispam software; and the use of access controls. Access controls include both physical access to CBSs, as well as access to authorized software via user and device authentication.

3.3. **Detect**. The detect element seeks to implement methods that recognize and identify inappropriate cyber activity within a CBS. Implementation technology includes monitoring the CBS with the ability to detect anomalies in system and network behavior and generate appropriate alarms. The detect element also includes verification that the CBS is correctly implementing security functions.

3.4. **Respond**. The respond element seeks to minimize the impact of a cyber event on system and network behavior and prevent the cyber event from impacting other CBSs. An incident response plan is a key component of this element. It should document the planned response to preserve as much system functionality as possible. The use of redundant systems is one technique for preserving system functionality. In some cases, local backup controls that are independent of the primary control system are required by the International Maritime Organization International Convention for the Safety of Life at Sea (SOLAS) regulations. It should also be possible to stop all networking communication into or outside of a security zone; the CBSs within the security zone should still be capable of operation. Should a cyber event prevent a CBS from accomplishing its intended functions, a means should be available to put the CBS or network into a mode to achieve a safe state; often this state is for the CBS to stop all normal functions.

The contents of the incident response plan are detailed in IACS UR E26:

> "The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin.
>
> The incident response plan shall, as a minimum, include the following information:
>
> - Breakpoints for the isolation of compromised systems;
> - A description of alarms and indicators signaling detected ongoing cyber events or abnormal symptoms caused by cyber events;
> - A 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, if any.
> - Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable;
>
> The Incident response plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it."

3.5. **Recover**. The recover element seeks to restore all CBSs and associated networks to normal operation. A recovery plan is an important element of the recover element. The recovery plan includes details on where assistance may be obtained and the organizations that should be involved in the recovery effort. It should also include data backup and restore practices to enable recovery. As detailed in IACS UR E26:

> "When developing recovery plans, the various systems and subsystems involved shall be specified. The following recovery objectives shall also be specified:

(1) 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.

(2) Data recovery: methods and procedures to recover data necessary to restore safe state of OT[1] systems and safe ship operation shall be specified in terms of Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential cyber incidents shall be created, and the recovery procedure developed and described. Recovery plans shall include, or refer to the following information;

(1) Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.

(2) Processes and procedures for the backup and secure storage of information.

(3) Complete and up-to-date logical network diagram.

(4) The list of personnel responsible for restoring the failed system.

(5) Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.

(6) Current configuration information for all components.

The operation and navigation of the ship shall be prioritized in the plan in order to help ensure the safety of onboard personnel.

Recovery plans in hard copy onboard and ashore shall be available to personnel responsible for cyber security and who are tasked with assisting in cyber incidents."

4. Cybersecurity operational impact

Cybersecurity should not be passive. Crew training is critical to ensuring safe cyber practices (protect element) are part of the organizational culture; short cuts (such as bypassing access controls) that create cyber vulnerabilities are not taken. The documentation supporting cybersecurity resilience, including inventories and plans should

[1] Operational Technology – Hardware, software, and networks that monitor and control onboard systems. (Defined in IACS UR E26).

be regularly reviewed and updated. Regular exercises should be carried out to train the crew on detecting, responding, and recovering from cyber incidents.

While the preparation for cyber incidents requires the investment of time and resources, the payoff is in fast recovery in response to a cyber incident. Lost operational time can be very expensive.

5. References

ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries, ABS CyberSafety Volume 2, June 2025.

IACS UR E26, Cyber resilience of ships

IACS UR E27, Cyber resilience of on-board systems and equipment

NIST, The NIST Cybersecurity Framework (CSF) 2.0, February 26, 2004. https://doi.org/10.6028/NIST.CSWP.29