ABS REGULATORY NEWS
No. 14/2023

IACS UNIFIED REQUIREMENTS ON CYBER RESILIENCE

This Regulatory News provides guidance on the two new IACS Unified Requirements (URs) that establish minimum goal-based requirements for cyber resilience of new ships and the cyber resilience of onboard systems and equipment.

KEY NOTES

Application:
These Unified Requirements are to be uniformly implemented by IACS Societies on ships contracted for construction on or after 1 July 2024 and may be used for other ships as non-mandatory guidance.

Effective date:
1 July 2024

References:

- IACS UR E26 Rev.1 – Cyber Resilience of Ships
- IACS UR E27 Rev.1 – Cyber Resilience of On-Board Systems and Equipment
- ABS Rules for Building and Classing Marine Vessels (MVR)
- ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries - ABS CyberSafety® Volume 2
- ABS Cyber Resilience Program
- ABS Notations and Symbols

INTRODUCTION

As technologies have expanded and automation systems have become more complex, the probabilities for cyber-attacks increase, along with their potential effects on personnel, data, safety of vessels, and the environment. The need for robust cybersecurity programs has become a critical component of the overall operations of marine assets.

Attackers may target any combination of people and technology to achieve their aim, wherever there is a network connection or any other interface between onboard systems and the external world. Safeguarding ships and shipping from current and emerging threats involves a range of measures that are continually evolving.

In April 2022, the International Association of Classification Societies (IACS) published the original versions of its Unified Requirements (UR) on cyber resilience:

- IACS UR E26 – Cyber Resilience of Ships
- IACS UR E27 – Cyber Resilience of On-Board Systems and Equipment

In September 2023, IACS announced their plan to issue revisions to URs E26 and E27 and to delay the implementation dates of the original documents.

Both URs were scheduled to have an entry into force date of January 1, 2024, for new construction vessels.

After publishing the original versions, IACS collected industry feedback and continued work to improve these URs. As a result, IACS recently published the Rev. 1 version of UR E27 in September 2023 and the Rev. 1 version of UR E26 in November 2023. The Rev. 1 versions of the URs are planned to come into effect on July 1, 2024.

To avoid confusion between the two versions of these URs, IACS has decided that the Rev. 1 versions will supersede the original versions. Therefore, the original versions will not enter into force. Only the Rev. 1 versions will enter into force and the entry in force date will be July 1, 2024.

APPLICATION

The Rev. 1 version of UR E26 indicates that the IACS unified requirements are applicable to the following vessels:

- Passenger ships (including passenger high-speed craft) engaged in international voyages.
- Cargo ships of 500 GT and upwards engaged in international voyages.
- High speed craft of 500 GT and upwards engaged in international voyages.
- Mobile offshore drilling units of 500 GT and upwards.
- Self-propelled mobile offshore units engaged in construction. (i.e. wind turbine installation maintenance and repair, crane units, drilling tenders, accommodation, etc.)

The IACS unified requirements may be used as non-mandatory guidance for any other type of vessel.

CYBER RESILIENCE AND THE IACS URS

These two IACS URs are based on the concept of Cyber Resilience.

Cyber Resilience

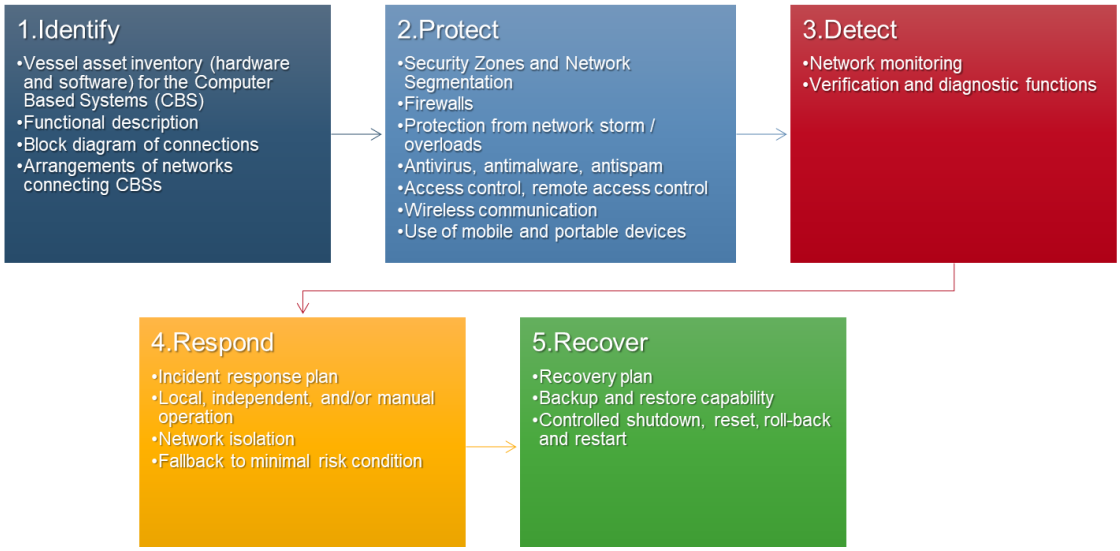
The capability to reduce the occurrence and mitigate the effects of cyber incidents arising from the disruption or impairment of operational technology (OT) used for the safe operation of a ship, which potentially lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

Cyber resilient vessels, systems and equipment have built-in defenses for cyber incidents and the vessel as well as the crew have measures in place for responding when a cyber incident occurs. The IACS URs were developed to establish a common set of minimum requirements to deliver a vessel that can be described as cyber resilient.

UR E26 Cyber Resilience of Ships

UR E26 aims to provide the minimum set of requirements for cyber resilience for the vessel. It is intended for the design, construction, commissioning and operational life of the ship. This UR covers five key functional aspects for cybersecurity: Identify, Protect, Detect, Respond, and Recover. The UR recognizes the different roles of the Suppliers, Integrators, Owners and Class Society.

UR E26 has 17 requirements organized according to the five key functional aspects for cybersecurity, and each of the 17 requirements includes a statement of the requirement, the rationale and an explanation of the requirement details.



Furthermore, the Rev.1 version of the UR includes information regarding demonstration of compliance for each of the IACS requirements (for example, during the construction phase, commissioning phase and annual surveys).

The UR also requires the Cyber Resilience Test Procedure to be developed for the vessel. The procedure would cover the testing during the construction phase and commissioning as well as during the annual surveys (i.e. operational life of the vessel).

UR E27 Cyber Resilience of On-board Systems and Equipment

UR E27 aims to provide the minimum-security capabilities for systems and equipment to be considered cyber resilient. It is intended for third party equipment suppliers.

Required documentation

- Computer Based Systems (CBS) Asset Inventory
- Topology Diagrams
- Document describing security capabilities
- Test Procedure of security capabilities
- Security configuration guidelines
- Secure Development Lifecycle (SDLC) documents
- Plans for maintenance and verification of the CBS
- Information supporting the owner's incident response and recovery plan
- Management of change plan
- Test reports

Early adopters (suppliers, integrators, and owners) can benefit from ABS services by getting systems and equipment certified early. By acting early your organization will be ready to provide services in line with upcoming requirements before the July 1, 2024, entry into force date.

If you have any questions or comments regarding the application of these requirements, please contact your local ABS office or send a message to RSD@eagle.org.

Regarding ABS certification for the UR E27 requirements, please also see our webpage for the *ABS Cyber Resilience Program* by using the following link.

Link:	https://ww2.eagle.org/en/Products-and-Services/vendor-certification/abs-cybersafety-for-resilience.html

REFERENCES

Document	Title
IACS UR E27 Rev.1	Cyber Resilience of On-Board Systems and Equipment
IACS UR E26 Rev.1	Cyber Resilience of Ships
ABS MVR	ABS Rules for Building and Classing Marine Vessels (MVR)
ABS Notations	ABS Notations and Symbols
ABS CyberSafety Volume 2	Guide for Cybersecurity Implementation for the Marine and Offshore Industries

World Headquarters
1701 City Plaza Drive | Spring, TX 77389 USA
P 1-281-877-6000 | F 1-281-877-5976
ABS-WorldHQ@eagle.org
www.eagle.org