



# CYBER RESILIENCE GUIDANCE

FOR EQUIPMENT PROVIDERS FOR  
MARINE AND OFFSHORE INSTALLATIONS

---

---

# TABLE OF CONTENTS

Introduction .....	1
When is Cyber Resilience Approval Required? .....	2
Approval Routes .....	3
System vs. Component Approval .....	3
Cyber Resilience in the ABS Rules .....	4
Insights for a Successful Submission .....	4
Frequently Asked Questions .....	5
Required Documentation for ABS Cyber Resilience PDA .....	8
Cyber Resilience Checklist (UR E27) .....	9

## INTRODUCTION

The International Association of Classification Societies (IACS) released Unified Requirement (UR) E27 addressing Cyber Resilience of On-Board Systems and Equipment, applicable to new construction ships (ships contracted for construction on or after July 1, 2024).

The purpose of IACS UR E27 is to confirm that equipment vendors and manufacturers have appropriate controls and safeguards in place to protect and strengthen system integrity. It addresses cyber resilience for onboard systems and equipment, user-computer system interfaces, and outlines product design and development requirements for implementing new devices on board.

To support acceptance of equipment on board vessels, ABS offers Product Design Assessments (PDAs) of equipment. This activity evaluates equipment for compliance with ABS Rules as well as national and international standards. With the development of cyber requirements, computer-based systems (CBS) are now required to meet UR E27 and IEC 62443 standards.

This document has been developed to assist equipment providers in understanding and complying with the UR E27 requirements.





---

## WHEN IS CYBER RESILIENCE APPROVAL REQUIRED?

The *ABS Rules for Building and Classing Marine Vessel (MVR) 4-9-13/5* and *4-9-14/5* outline the systems that are subject to cyber resilience requirements.

The requirements focus on operational technology (OT) systems on board ships – specifically, control and monitoring systems that utilize data to manage physical processes. These systems can be susceptible to cyber incidents. If compromised, they may result in dangerous situations that pose risks to human safety, the integrity of the vessel and the environment.

Therefore, approval is required for CBS used for systems such as:

- Propulsion
- Steering
- Anchoring and mooring
- Electrical power generation and distribution
- Fire detection
- Fire extinguishing
- Bilge and ballast
- Loading computer
- Watertight integrity and flooding detection
- Lighting (e.g., emergency lighting, low locations and navigation lights)
- Any required safety system whose disruption or functional impairment may pose risks to vessel operations (e.g., emergency shutdown system, cargo safety system, pressure vessel safety system and gas detection system)
- Navigational systems required by statutory regulations
- Internal and external communications systems required by ABS and statutory regulations

For navigation and radiocommunication systems, the application of IEC 61162-460, or other equivalent standards, may be accepted as an alternative to the required security capabilities in *MVR 4-9-14/15*, provided that they meet the requirements outlined in *MVR 4-9-13*.

The approval must also be considered for any internet protocol (IP)-based communication interface from CBS in scope to other systems.

## APPROVAL ROUTES

Route	Description
<b>Individual Project (vessel) Approval</b>	Approval for each vessel-specific installation. Requires full documentation review and a survey.
<b>Type Approval/Product Design Assessment (PDA)</b>	Approval for standard products. Allows for a one-time review of the product to facilitate subsequent installation on board vessels. This reduces the documentation and survey burden.

## SYSTEM VS. COMPONENT APPROVAL

To streamline cyber resilience compliance across multiple systems, ABS allows for flexibility in how cyber resilience PDAs are issued. If multiple systems or components share the same cyber resilience architecture, such as identical network topologies, access controls and vulnerability mitigation strategies, it is efficient and acceptable to issue a standalone cyber resilience PDA that covers only the relevant aspects. This standalone PDA can then be referenced by other PDAs for individual systems, helping to avoid duplication of effort and maintain consistency in cyber resilience documentation and review.

This approach is particularly useful for original equipment manufacturers (OEMs) that produce a family of products or systems relying on a common cyber resilience framework. By issuing a dedicated cyber resilience PDA, the OEM can demonstrate that the shared design has been reviewed and approved by ABS. Each system-specific PDA can then reference this cyber resilience PDA, reducing the documentation burden and simplifying the approval process.

Alternatively, an existing PDA can incorporate the cyber resilience review, which addresses controls, automation or electrical suitability aspects for a specific system. This is appropriate when the cyber resilience design is unique to that system or when the OEM prefers to consolidate all compliance documentation into a single submission. In this case, the PDA will include the functional and cyber resilience evaluations, and the ABS certificate will reflect compliance with requirements.

Both approaches are valid and recognized by ABS. The choice depends on the OEM's product structure, documentation strategy and whether the cyber resilience design is shared or system specific. In either case, the PDA must meet all requirements outlined in the ABS Rules.

This needs to be specified during the PDA request stage in the extra comments section for clarity.



## CYBER RESILIENCE IN THE ABS RULES

The ABS Rules addressing cyber resilience requirements applicable to vessels and onboard systems can be accessed on the ABS website at [www.eagle.org](http://www.eagle.org).

Specifically, the ABS MVR includes comprehensive cyber resilience requirements in Part 4, Section 14, Cyber Resilience for Onboard Systems and Equipment.

This section aligns with the UR E27 requirements and outlines the mandatory cyber resilience measures for CBS installed on vessels contracted for construction on or after July 1, 2024, which are required to get the Cyber Resilience (CR) notation.

To access these Rules:

1. Visit the ABS Rules and Guides page on [www.eagle.org](http://www.eagle.org).
2. Search for the *ABS Rules for Building and Classing Marine Vessels – 2025*.
3. Navigate to Part 4, Section 14 (or 4-9-14) to find the cyber resilience requirements.

This section details the scope of applicability, documentation requirements, system-level security capabilities, secure development life cycle expectations and survey procedures. It also includes criteria for risk-based exclusions.

In addition to the Rules, ABS provides supporting guidance documents and templates to help OEMs and shipowners comply with cyber resilience requirements.

For the most current and official information, refer to the ABS website and the latest version of the ABS MVR.

---

## INSIGHTS FOR A SUCCESSFUL SUBMISSION

- Clearly label all documents with version numbers and system identifiers.
- Ensure all required documents are submitted.
- Avoid statements like “Doesn't Apply” or “N/A.” Instead, provide an explanation why a specific requirement is not applicable.
- Describe your product in detail.
- Cyber resilience compliance may be incorporated into the product's initial PDA certificate. This will revalidate the certificate, covering all the applicable requirements of the ABS Rules. Alternatively, indicate in the PDA request stage if the certification scope will be limited to cyber resilience compliance only, in case there are already other ABS PDA certificates covering additional requirements of the product and application.
- Use the check sheets below to aid with submission.
- Complete the ABS PDA Request form on the ABS website to start the process.

---

## FREQUENTLY ASKED QUESTIONS

The purpose of this section is to offer general advice and responses to inquiries that are commonly directed to ABS. For inquiries that are particularly specific, clients are advised to contact ABS using the contact information provided on the last page to obtain guidance tailored to their individual circumstances. Regarding matters associated with CBS exclusions, it is recommended that they be addressed on a case-by-case basis.

### IS COMPLIANCE WITH UR E26 AND UR E27 REQUIRED FOR A FULLY ISOLATED SYSTEM?

If a CBS is completely independent, with no internet connection, no physical interfaces (e.g., USB, CD drive) and no links to external systems, it is not required to comply with UR E26 and UR E27.

Additionally, if the system falls under the categories listed in the ABS MVR 4-9-13/5.1, the exclusion evaluation in ABS MVR 4-9-13/17 may apply.

### DO “HUMAN USERS” IN UR E27 REV.1 (SECTION 4/REQUIREMENT NO.1) INCLUDE COMMISSIONING ENGINEERS?

Yes. The term “human users” includes crew members and commissioning engineers. This definition covers all individuals who interact with the system, from commissioning through operation, to help ensure safety and usability throughout its life cycle.

### IF MY SYSTEM INCLUDES HARDWARE FROM ANOTHER VENDOR, DO THOSE COMPONENTS NEED TO MEET THE REQUIRED SECURITY CAPABILITIES?

Yes. According to the definition of “System” in UR E27 (Section 1.4), a system is a combination of interacting programmable devices and/or sub-systems organized to achieve one or more specified purposes. Therefore, any third-party equipment within the system’s scope must also demonstrate compliance.

The supplier or manufacturer of that equipment should provide evidence of meeting the required security capabilities.

### IS UR E10 AND UR E22 APPROVAL A PREREQUISITE FOR UR E27 APPROVAL?

No, **UR E10 and UR E22 are not within the scope of UR E27**. However, they are expected to be applied as relevant for classification purposes. Specifically:

- **UR E10** addresses environmental performance of system hardware.
- **UR E22** covers safety and functionality of software and hardware in CBS.

If you’re applying for or revalidating a PDA certificate, it’s recommended to **combine compliance with UR E10, E22 and E27** to help ensure full alignment with classification requirements.

### DOES A LAYER 2 (L2) SWITCH REQUIRE UR E27 APPROVAL?

If the **L2 switch** is part of a system that manages communication either within the applicable system or with external systems, then **UR E27 approval is required**.

However, if the L2 switch is an **unmanaged switch**, meaning it does not have configuration capabilities or software-based control, then **UR E27 approval is not required**.

### IS THERE A TEMPLATE OR SAMPLE FORMAT FOR DOCUMENTS REQUIRED UNDER UR E27?

Yes. Refer to the check sheet and templates provided at the end of this document.

**WHEN IS SUBMISSION OF DOCUMENTATION TO ABS REQUIRED UNDER UR E27 SECTION 3.1?**

Submission is required during the supplier approval phase for the following documents:

- Secure development lifecycle documentation (Section 3.1.5)
- Maintenance and verification plans for the CBS (Section 3.1.6)
- Information supporting the owner's incident response and recovery plan (Section 3.1.7)
- Management of change plan (Section 3.1.8)

**IS A QUALIFIED PERSON OR PRE-CERTIFICATION REQUIRED TO PERFORM UR E27 TESTING?**

No. UR E27 does not require the use of a qualified person or a certified testing organization to carry out tests for secured capabilities.

**WHEN IS UR E27 APPROVAL NOT REQUIRED FOR SYSTEMS ON SHIPS WITH ABS NOTATION CR?**

UR E27 approval is generally not required under the following conditions:

- The system is not a CBS.
- It is a CBS but does not qualify as an applicable OT system.
- It is a CBS and qualifies as an applicable OT system but is exempted under ABS MVR 4-9-13/17.5 (refer to Chapter 6 of E26).

**IS UR E27 APPROVAL REQUIRED FOR A STANDALONE COMPONENT WITHIN A CBS (E.G., A GENERAL-PURPOSE PROGRAMMABLE LOGIC CONTROLLER)?**

Yes. A standalone component can receive UR E27 approval. However, the entire configured CBS must also be evaluated and approved under UR E27.

**DOES CONNECTING A SERVICE ENGINEER'S LAPTOP TO AN OT SYSTEM DURING MAINTENANCE CLASSIFY THE OT SYSTEM AS CONNECTED TO AN UNTRUSTED NETWORK?**

No. A service engineer's work computer that is used temporarily for maintenance is **not considered an "other system"** under UR E26 Section 1.3.2.

- The approved service engineer from the supplier is to implement appropriate cybersecurity measures for their laptop connection.
- The OT system is not classified as connected to an untrusted network in this scenario.

The approved service engineer from the supplier is to implement appropriate cybersecurity measures for their laptop connection.

**DOES A FIREWALL REQUIRE UR E27 APPROVAL?**

Yes. If the firewall controls communication within the applicable system or with external systems, it must comply with UR E27.

**HOW DOES ABS VERIFY COMPLIANCE WITH UR E26 AND UR E27 FOR NAVIGATION AND RADIOCOMMUNICATION SYSTEMS GOVERNED BY STATUTORY REGULATIONS?**

These systems are typically **not submitted to class for review**. However, compliance is expected through alternative standards such as:

- IEC 61162-460
- IEC 63154

These standards must provide cyber resilience equivalent to or greater than that required by UR E26 and UR E27.

**ARE CLIENTS REQUIRED TO SUBMIT PROPRIETARY SOFTWARE DETAILS (E.G., OPERATING SYSTEMS, DATABASES, CONFIGURATION FILES) FOR UR E27 REVIEW?**

No. ABS **does not require submission of actual software code or proprietary functionality**.

References to databases and protocols in UR E27 are intended for informational purposes only (e.g., listing the types of software used) and not for detailed review of their internal workings.

This approach respects intellectual property concerns while still supporting cybersecurity evaluation.



## REQUIRED DOCUMENTATION FOR ABS CYBER RESILIENCE PDA

Document	Purpose	Document ID/Name
<b>CBS Asset Inventory</b>	Lists all hardware/software components, versions and interfaces.	
<b>Topology Diagrams</b>	Shows physical and logical network architecture.	
<b>Security Capabilities Description</b>	Maps system features to UR E27 requirements.	
<b>Test Procedures</b>	Defines how security features are verified.	
<b>Security Configuration Guidelines</b>	Recommends secure settings and default values at the time of the integration.	
<b>Secure Development Life Cycle (SDLC)</b>	Describes how security is managed during development.	
<b>Maintenance and Verification Plan</b>	Explains how users can verify security functions.	
<b>Incident Response Support</b>	Provides procedures for backup, restoration, isolation, etc.	
<b>Change Management Plan</b>	Describes how updates and changes are controlled.	
<b>Test Reports</b>	Required to demonstrate successful testing if following the type approval route.	

## CYBER RESILIENCE CHECKLIST (UR E27)

The CBS must implement or justify compensating controls and demonstrate SDLC requirements for the following items.

Requirements		Document Number	Notes	ABS Notes
<b>Access Control and Authentication</b>				
1	Human user identification and authentication			
2	Account management			
3	Identifier management			
4	Authenticator management			
5	Wireless access management			
6	Strength of password-based authentication			
7	Authenticator feedback			
<b>Audit and Monitoring</b>				
8	Authorization enforcement			
9	Wireless use control			
10	Use control for portable and mobile devices			
11	Mobile code			
12	Session lock			
13	Auditable events			
14	Audit storage capacity			
15	Response to audit processing failures			
16	Timestamping			

Continued on next page.

Continued from previous page.

Requirements		Document Number	Notes	ABS Notes
<b>Data Protection</b>				
17	Communication integrity			
18	Malicious code protection			
19	Security functionality verification			
20	Deterministic output			
<b>System Resilience</b>				
21	Information confidentiality			
22	Use of cryptography			
23	Audit log accessibility			
24	Denial of service protection			
25	Resource management			
26	System backup			
27	System recovery and reconstitution			
28	Alternative power source			
29	Network and security configuration settings			
30	Least functionality			

Continued on next page.

Continued from previous page.

Requirements		Document Number	Notes	ABS Notes
<b>Untrusted Network Controls (if applicable)</b>				
31	Multifactor authentication for human users			
32	Software process and device identification and authentication			
33	Unsuccessful login attempts			
34	System use notification			
35	Access via untrusted networks			
36	Explicit access request approval			
37	Remote session termination			
38	Cryptographic integrity protection			
39	Input validation			
40	Session integrity			
41	Invalidation of session IDs after session termination			
<b>SDLC Requirements</b>				
42	Private key management			
43	Security update process			
44	Compatibility with operating system/ component updates			
45	Defence-in-depth strategy			
46	Hardening guidelines			

---

# CONTACT INFORMATION

## GLOBAL SUSTAINABILITY CENTER

1701 City Plaza Dr.  
Spring, Texas 77389, USA  
Tel: +1-281-877-6000  
Email: [Sustainability@eagle.org](mailto:Sustainability@eagle.org)

## NORTH AMERICA REGION

1701 City Plaza Dr.  
Spring, Texas 77389, USA  
Tel: +1-281-877-6000  
Email: [ABS-Amer@eagle.org](mailto:ABS-Amer@eagle.org)

## SOUTH AMERICA REGION

Rua Acre, n° 15 - 11° Floor, Centro  
Rio de Janeiro 20081-000, Brazil  
Tel: +55 21 2276-3535  
Email: [ABSRio@eagle.org](mailto:ABSRio@eagle.org)

## EUROPE REGION

111 Old Broad Street  
London EC2N 1AP, UK  
Tel: +44-20-7247-3255  
Email: [ABS-Eur@eagle.org](mailto:ABS-Eur@eagle.org)

## AFRICA AND MIDDLE EAST REGION

Al Joud Center, 1st floor, Suite # 111  
Sheikh Zayed Road  
P.O. Box 24860, Dubai, UAE  
Tel: +971 4 330 6000  
Email: [ABSDubai@eagle.org](mailto:ABSDubai@eagle.org)

## GREATER CHINA REGION

World Trade Tower, 29F, Room 2906  
500 Guangdong Road, Huangpu District,  
Shanghai, China 200000  
Tel: +86 21 23270888  
Email: [ABSGreaterChina@eagle.org](mailto:ABSGreaterChina@eagle.org)

## NORTH PACIFIC REGION

11th Floor, Kyobo Life Insurance Bldg.  
7, Chungjang-daero, Jung-Gu  
Busan 48939, Republic of Korea  
Tel: +82 51 460 4197  
Email: [ABSNorthPacific@eagle.org](mailto:ABSNorthPacific@eagle.org)

## SOUTH PACIFIC REGION

7 Science Park Drive #09-21/32  
Geneo, Singapore 119316  
Tel: +65 6276 8700  
Email: [ABS-Pac@eagle.org](mailto:ABS-Pac@eagle.org)

© 2025 American Bureau of Shipping.  
All rights reserved.

