The real cyber risk in ship equipment that CVE counts alone do not show

94% of recent marine equipment risk assessments were at a level requiring cyber risk treatment to be considered

CYTUR

CYTUR Inc. | www.cytur.net | info@cytur.net
Published September 2026

Prologue.

What mattered more than the number of vulnerabilities was the actual risk

When people discuss the cybersecurity of ship equipment, the first thing usually checked is CVEs. How many known vulnerabilities are there, are any of them high severity, and has the latest security patch been applied. CVEs are an important starting point for understanding the security posture of a piece of equipment.

But does a higher CVE count always mean higher actual cyber risk?

When CYTUR re-examined the results of more than a dozen recent marine equipment cyber risk assessments, risks that could not be explained by CVE counts alone were found repeatedly in the field.

94% of the systems assessed were rated **Appropriate or Required** under International Association of Classification Societies (IACS) Recommendation 171, meaning that risk treatment should be appropriately considered or is required. **About 60%** of the systems assessed were rated Required, meaning that risk treatment is mandatory.

The part of this data that deserves more attention, however, is something else. The reason for the high risk levels was not simply that there were many CVEs.

What determined the risk level was a combination of factors: what the system was connected to, which ports and services were actually active, the state of its software and firmware, and what a compromise would mean for the operation of the vessel.

This brief uses data from scanning and assessing real equipment to answer one question.

> **What actually determines the cyber risk of ship equipment?**

To answer it, we look in turn at five findings that appeared repeatedly in the data.

94%	94% of the systems assessed were at a level requiring risk treatment to be considered, and about 60% were rated Required, where treatment is mandatory.
10x, same rating	One system had more than 200 CVEs and another had about 20, yet both were rated Required.
8 open ports	On equipment that communicates only over serial links, 8 service ports were open on the Ethernet side, and the same structure appeared at two different equipment manufacturers.
0 vs 13	The manufacturer’s own core controller had zero CVEs while the network device installed alongside it had 13. Vulnerabilities were concentrated in the bundled components.
20 to 12	After re-verifying the implemented measures and the network isolation state, the Risk Level fell from 20 to 12. In one case the retest was passed three weeks later.

1. What 94% tells us

One thing must be clarified before interpreting the 94% figure. It does not mean that 94% of the equipment assessed had vulnerabilities.

The IACS Rec 171 risk assessment does not calculate a Risk Level from the presence or absence of CVEs alone. It considers Category, which reflects the criticality of the system, Impact in the event of an incident, and Likelihood, which reflects the probability of attack. Because of this structure, systems that directly affect ship safety start out with a certain minimum Risk Level. For example, a Category 3, Impact 4 system cannot fall into the Optional range even at the lowest possible Likelihood.

The 94% figure should therefore not be read as meaning that the equipment was that vulnerable.

Risk Treatment	Risk Level	Meaning
Optional	RL < 4	Treatment considered optional
Appropriate	4 ≤ RL ≤ 12	Treatment appropriately considered
Required	RL > 12	Treatment required

[Table 1] IACS Rec 171 risk treatment criteria

Even so, what stands out in these results is clear.

94% Risk treatment to be considered

Required: RL > 12 Appropriate: 4 ≤ RL ≤ 12 Optional: RL < 4

[Figure 1] Distribution of risk treatment ratings under IACS Rec 171 | Source: CYTUR

System criticality alone did not determine these results. What separated the Risk Levels among the systems assessed was Likelihood, and what determined Likelihood was the network connection structure and the active interfaces and services, in other words the attack surface formed in the real operating environment.

The key question this data addresses is not whether risk exists, but **what makes risk higher in the real operating environment**.

2. The CVE counts differed by more than ten times, yet both were Required

One comparison among the assessment results is worth noting.

In one Integrated Automation System (IAS), **more than 200 CVEs** were found to apply. In another Integrated Automation System, **about 20 CVEs** were identified. The CVE counts differed by more than ten times.

Yet the risk assessment results were **Risk Level 20** and **Risk Level 16** respectively, and both systems were rated Required.

	System A	System B
CVEs identified	**More than 200**	**About 20**
Risk Level	**20**	**16**
Rating	**Required**	**Required**

[Table 5] Assessment results of two Integrated Automation Systems (IAS) | Source: CYTUR

It is easy to assume that fewer CVEs means proportionally lower risk. This case shows otherwise. The system with about 20 CVEs was rated Required, exactly as the system with more than 200 was.

> **CVE count and cyber risk are not the same metric.**

A CVE count shows how many known technical vulnerabilities exist. The urgency and scope of treatment, however, were determined by whether those vulnerabilities could actually be reached, whether a path existed to other systems, and what a compromise would mean for the operation of the vessel. What mattered was not how many vulnerabilities existed, but which vulnerabilities connected to a real attack path.

3. Risk was also being created outside the CVE list

3-1. Documented as unused is not the same as actually disabled

The network configuration information provided by the equipment manufacturers did not match the active ports and services found in the actual scans.

On one piece of equipment whose primary communication is serial (RS-485), **8 service ports were found active** even though the Ethernet interface was not in use. The types of service found active were as follows.

Service identified	Function or purpose
Engineering communication	Uploading and downloading PLC programs
Server communication	Sending and receiving control commands
Printer service	Found active on the Ethernet side, which is not used for primary communication

[Table 2] Types of active service found on the Ethernet side of serial-communication equipment | Source: CYTUR

This pattern did not appear in only one place. **The same structure was found in the systems of two different equipment manufacturers.** Both systems used the same family of PLC and HMI, and the Ethernet-side services on equipment that communicates only over serial links were left open.

The presence of these services does not by itself mean the equipment is vulnerable. But every unnecessary port and service that is active increases the number of paths an attacker could use. The PLC engineering port in particular can become a channel for attempts to make unauthorized program changes.

The important question is not only whether a service is being used. It is **whether, if it is not used, it has actually been disabled**.

> **An unused door is not a locked door.**

3-2. Vulnerabilities were in the bundled components rather than in the equipment itself

Marine equipment is never a single device. Industrial switches, firewalls, general purpose operating systems, web servers, off the shelf PLCs and HMIs, and other third party components together form one system.

In one assessment, the **core controller built by the equipment manufacturer had zero public CVEs**. The **web management function of the industrial network device installed alongside it had 13 CVEs**, because the scripting engine behind that web interface was an outdated version.

In other assessments as well, vulnerabilities were found in the general purpose components. In one system, **80 CVEs** were identified in the bundled off the shelf PLC, HMI and I/O modules, and in another, **37 CVEs** were identified in the firewall operating system.

Assessment	Component	CVEs identified
Case A	Core controller built by the equipment manufacturer	0
Case A	Web management function of the industrial network device	13
Case B	Off the shelf PLC, HMI and I/O modules	80
Case C	Firewall operating system	37

[Table 3] Components and CVE counts by assessment | Source: CYTUR

This means that checking a single product name is not enough when looking at equipment cybersecurity. What actually needs to be examined is **the full combination of hardware, software and firmware that makes up the equipment**. This is why IACS UR E27 requires the asset inventory to include not only hardware but also software, firmware, interface and protocol information.

3-3. Vulnerabilities disclosed years earlier were still present

Another issue found repeatedly was the lifecycle of software and firmware.

Operating systems that have reached end of support, and therefore no longer receive new security patches, were found on **three or more different pieces of equipment**. They varied in type, from an embedded Windows family to a mobile operating system family to a server Linux distribution. One of them had already reached end of official support five years before the assessment.

In addition, there were cases where **vulnerabilities whose security advisories had been published more than three years earlier** were found unchanged in new assessments. The advisory and the patch existed, but the equipment had been installed without them.

Ship equipment stays in service for a long time once installed. The security state of its software and firmware, however, keeps changing. A version that was sound at delivery may see new vulnerabilities disclosed during the vessel's operating life, and in some cases

an already outdated version was installed at the time of delivery.

Equipment cybersecurity therefore cannot end with a one time check at delivery.

Know the asset, know the version, and keep matching them against newly disclosed vulnerabilities.

4. Four factors determined the actual cyber risk

Vulnerability, exposure, connectivity, impact

Taken together, the assessment results show that four factors had to be considered together to understand the actual risk.

*The four factors below do not replace the IACS Rec 171 formula (Risk Level = 2 × (Category + Likelihood + Impact − 4)). They explain how the values that go into that formula are determined on real equipment. Exposure and connectivity are elements that make up Likelihood, and impact corresponds to Impact in the formula.

1. Vulnerability
Check whether known CVEs exist. That alone, however, is not enough.

2. Exposure
Check which ports and services are actually active, and whether authentication and encryption are applied.

3. Connectivity
Check which networks the equipment is connected to, and whether a path exists to other onboard systems.

4. Impact
Judge what effect a compromise of the system would have on the operation, safety and environmental performance of the vessel.

Viewed together, these four factors reveal differences that a CVE list alone does not show. Even where many known vulnerabilities exist, the probability of attack can be lower if actual access is restricted. Conversely, even with relatively few CVEs, the Risk Level rises if a remote management function is open, the system is directly connected to other major systems, and it serves a core function of the vessel.

Where a vulnerability scan asks which vulnerabilities exist, a risk assessment goes one step further and asks what risk those vulnerabilities could create on the actual vessel.

5. The risk could be reduced

The result of re-verifying the implemented measures and the network state, then recalculating the risk

The purpose of a risk assessment is not to find as many risks as possible. It is to actually reduce them.

In one case where CYTUR performed a retest, the initial assessment rated the system **Risk Level 20, Required**. The equipment manufacturer then implemented improvements, including software and firmware updates, shutdown of unnecessary file transfer and remote call services, and conversion of the management interface to encrypted communication with authentication.

The same system was then scanned again. Rather than reviewing a statement that the measures had been completed, the actual network state was measured a second time.

Stage	Measures or verification
Improvement	Software and firmware updates, shutdown of unnecessary file transfer and remote call services, conversion of the management interface to encrypted communication with authentication
Retest	Verification that the recommended services had actually been shut down, that the system operates on a closed network isolated from external networks, and that its configuration had stabilized
Recalculation	The attack surface and Likelihood were recalculated to reflect the verified network state

[Table 4] Measures and verification steps in the retest case | Source: CYTUR

What changed: recommended services verified as shut down · closed network operation verified · attack surface and Likelihood recalculated

[Figure 2] Change in risk level before and after the retest | Source: CYTUR

The important point is that the Risk Level did not simply drop because a few ports were closed. The risk was recalculated only after verifying that the security measures were actually in place, what network environment the system operates in, and whether the attack surface had actually been reduced.

This was not an isolated case. **In multiple retest cases, implementation of the recommended measures was verified**, including firmware updates, shutdown of

unnecessary services and disabling of unused interfaces. In one of them, a retest **three weeks after the assessment report was issued** confirmed that every vulnerability identified in the initial assessment had been mitigated. Where exactly what needed fixing was specified, equipment manufacturers were able to move quickly.

Not every risk disappeared, however. In some cases a service was disabled but its port remained open, and in another a remote display protocol required for operation remained, with the structural limitation that it communicates in plaintext. Such items were identified and managed as **residual risk** after verifying the operating condition of a closed network isolated from external networks.

The goal of cybersecurity is not to force risk to zero.

> **Know what remains, be able to explain why it was accepted, and keep managing that state.**

6. What these results mean for shipowners, shipyards and equipment manufacturers

The same data leaves a different question with each of the three parties

Shipowners and ship managers

Before the CVE count of the equipment being delivered, the first thing to ask about is the inventory: whether hardware, software and firmware versions and the list of active ports exist as documentation, and whether that documentation matches what is measured. New vulnerabilities continue to be disclosed during operation, so a framework for periodically updating the assessment made at delivery is needed.

- Obtain an asset inventory for each item of equipment before delivery (hardware, software, firmware, active ports)
- Set priorities by exposure, connectivity and impact rather than by CVE count
- Establish a cycle for periodic reassessment during the operating phase

Shipyards

Integration is the last opportunity to verify that systems that should be isolated by design are actually isolated. The default settings of equipment delivered by manufacturers, and in particular whether unused ports and services remain open, can only be confirmed by measurement. The documentation required by IACS UR E26 and E27 carries weight when it is supported by this measured data.

- State disabling of unused ports and services and firmware currency in the equipment delivery conditions
- Verify the difference between design and reality through measured scans during integration and sea trials
- Verify the results of corrective action by re-measurement rather than by a statement of completion

Equipment manufacturers (OEM)

In this data, vulnerabilities were concentrated not in the controllers built by the equipment manufacturers but in the switches, operating systems and off the shelf PLCs and HMIs that were bundled with them. The security of a product includes the security of its purchased components. At the same time, the retest cases show that where exactly what needs fixing is specified, the risk level can be lowered within weeks.

- Maintain a software bill of materials (SBOM) covering both in-house products and bundled components

- Check unused ports, services and management interfaces in the default configuration before shipment
- Provide post-remediation verification results to shipyards and shipowners as supporting evidence

7. From finding CVEs to managing actual risk

What 94% showed was not a simple vulnerability statistic

In more than a dozen recent marine equipment risk assessments performed by CYTUR, 94% were rated at a level where risk treatment should be appropriately considered or is required. About 60% of the systems assessed were rated Required.

The more important fact this data revealed, however, is something else. Actual risk was not explained by a single CVE number.

- Unused services were left open, and the same pattern repeated across different equipment manufacturers.
- Major vulnerabilities were concentrated in bundled third party components rather than in the core function of the equipment.
- End of support operating systems and vulnerabilities disclosed years earlier were found unchanged in new assessments.
- And where exactly what to fix was specified, the risk was actually reduced.

What determined the actual risk was the combination of vulnerability, exposure, connection structure and system impact.

In ship equipment cybersecurity, the question must not end at how many CVEs there are. The next question matters more.

> **"What risk could this vulnerability create on the actual vessel?"**

CYTUR Approach

From vulnerability detection to actual risk judgment and verification

CYTUR-SC scans real equipment and shipboard networks to identify assets, software and firmware, active ports and services, and known vulnerabilities. CYTUR analyzes this data together with the system's connection structure, operating environment and impact to assess the actual cyber risk under IACS Rec 171. After improvements are made, the same environment is checked again to verify whether the security measures are actually in place, how much the risk has been reduced, and what residual risk remains.

From simply finding vulnerabilities to judging and managing actual risk, CYTUR-SC.

About the data in this brief

This brief analyzes the results of more than a dozen recent equipment level cyber risk assessments performed by CYTUR, reclassified under the same IACS Recommendation 171 risk treatment criteria.

Method

Rather than reviewing drawings and documents, the CYTUR-SC scanner was connected to the actual equipment network to measure assets, firmware versions, active ports and services, and communication protocols. Identified assets were matched against public CVE databases.

Scope

Systems from more than ten equipment manufacturers across six categories: power and propulsion control, safety and emergency shutdown, automation and integrated control, HVAC, navigation and communication, and shipboard IT. The scope was not limited to any single equipment type.

Risk level calculation

The IACS Rec 171 formula (Risk Level = 2 × (Category + Likelihood + Impact − 4)) and treatment criteria (RL < 4 Optional, 4 ≤ RL ≤ 12 Appropriate, RL > 12 Required) were applied.

Limitations of the sample

The systems assessed were those commissioned for assessment by CYTUR's clients and are not a random sample representative of all marine equipment. The 94% figure must therefore not be read as meaning that 94% of all marine equipment is at risk. The figures in this brief describe patterns observed repeatedly in real operating environments, not safety judgments about individual products.

Anonymity

Individual clients, vessels, equipment manufacturers and product models are not disclosed.

About CYTUR

CYTUR Inc. is a cybersecurity company dedicated to ships and marine equipment. From threat modeling (TM) at the design stage, through security assessment (SC) and software bill of materials (SBOM) at the construction and delivery stages, to intrusion detection (MG) and threat intelligence (TI) during operation, CYTUR supports cyber resilience across the full vessel lifecycle. CYTUR products and services have obtained class approvals including ClassNK, RINA and KR, and are validated in real shipboard environments together with shipyards, equipment manufacturers and shipping companies in Korea and abroad.

CYTUR Inc.
Head office: A-2801, 97 Centum jungang-ro, Haeundae-gu, Busan, Republic of Korea
Seoul office: 901-910, Gasan KS Tower, 30 Beotkkot-ro 36-gil, Geumcheon-gu, Seoul, Republic of Korea
info@cytur.net | www.cytur.net

This brief is published by CYTUR for informational purposes and reflects the information available and CYTUR's professional judgment at the time of writing. The maritime industry and the cybersecurity environment change rapidly, and new vulnerabilities or threats may emerge after publication. This brief is not the result of a security audit of any specific product or system and may not be construed as legal or professional advice. Responsibility for decisions and actions taken on the basis of this brief rests with the user, and CYTUR accepts no liability for any resulting loss or damage. This brief may be cited provided the source is stated. © 2026 CYTUR Inc. All rights reserved.