Wärtsilä Cyber services

Managing cyber security risks in the marine environment

With vessels increasingly using systems that rely on digitalisation, integration and automation, cyber security risk management is a growing concern in the marine industry. As onboard information technology (IT) and operational technology (OT) is networked together and connected to the internet, the risk of unauthorised access and malicious attacks against a vessel's systems and networks is growing. It is now more important than ever that vessel owners and operators have a reliable partner with the right know-how to ensure uninterrupted operation and safety.

Cyber security in the marine industry

Cyber security is being recognised as an increasingly important factor in the reliable and safe operations of a connected maritime industry. As an evolution of the earlier IMO resolution to incorporate cyber risk management in the Safety Management System (SMS), new regulations and requirements are being progressively enforced. The IACS UR E26 and E27 requirements are being mandatory compliance requirements from Jan 2024 onwards.

Our solution

Wärtsilä monitors and supports the ongoing global cyber security standardisation, and targets meeting the relevant standards and legislation to safeguard our products and service operations throughout their lifecycle.

All Wärtsilä Cyber services are designed according to best practices and are based on the international IEC 62443 cyber security standard. Our services follow guidance on cyber security for the marine industry including:

- **ABS**: Guidance notes on the Application of Cybersecurity Principles to Marine and Offshore Operations
- **BIMCO**: Guidelines on Cyber Security Onboard Ships
- **DNV**: Recommended Practice for Cyber Security Resilience Management
- **IACS UR E27**: Cyber resilience of on-board systems and equipment
- **IET**: Code of Practice, Cyber Security for Ships
- **IMO MSC-FAL.1**: Guidelines on Maritime Cyber Risk Management
- **IMO MSC.428(98)**: Maritime Cyber Risk Management in Safety Management Systems

With Wärtsilä Cyber services, we help you to develop the resilience required to defend against and recover from any form of cyber interference. Wärtsilä Cyber services enable you to understand the current cyber security status of your operational environment and provide actions to mitigate identified cyber risks. Our services are designed to give a systematic 360-degree approach to cyber security risk mitigation, from assessing your current cyber posture to implementing cyber controls and lifecycle services

Wärtsilä Cyber services

Maintaining cyber resilience is a continuous process that should never be thought of as completed. Wärtsilä Cyber services consist of four modules that should be continuously applied to increase your cyber defence.

Cyber assessment

Assess your current situation and understand where you are in terms of cyber risks, compliance gaps or technical vulnerabilities.

Wärtsilä ICS risk assessment
Identify your critical assets and understand your related cyber maturity level by revealing cyber risks, possible compliance gaps and technical vulnerabilities.

Wärtsilä ICS vulnerability assessment
Protect your industrial control systems (ICS) and operational technology (OT) environment by identifying and validating security vulnerabilities related to external connections and internal systems.

Wärtsilä ICS asset visualisation
Obtain visibility into your OT assets and enhance your capability to proactively access cyber risks on an asset-to-asset basis.

Cyber recovery

Effective incident response is extremely important in the context of cyber resilience. As a leading maritime original equipment manufacturer (OEM) and service provider, we are a right partner for supporting and orchestrating incident response through our PSIRT (product security incident response team) and global service networks.

Cyber foundation

Establish the foundation for your cyber risk management by setting up a cyber security management system, governance and policies.

Wärtsilä ICS security foundation
Establish or improve your ICS cyber security setup by finding the set of policies, standards, industry best practices and rules that best serve your overall risk management strategy.

Cyber protection

Implement procedural and technical controls and system upgrades to reduce cyber risks.

Wärtsilä ICS vulnerability advisory
Receive notifications and guidance on threats and vulnerabilities for specific OT assets along with actionable recommendations to control and mitigate them.

Wärtsilä ICS patch validation
Obtain information about validated and approved security updates for your specific OT assets.

Wärtsilä ICS patch deployment
Ensure that your specific OT assets are equipped with the latest security updates to protect against cyber threats and to comply with regulations.

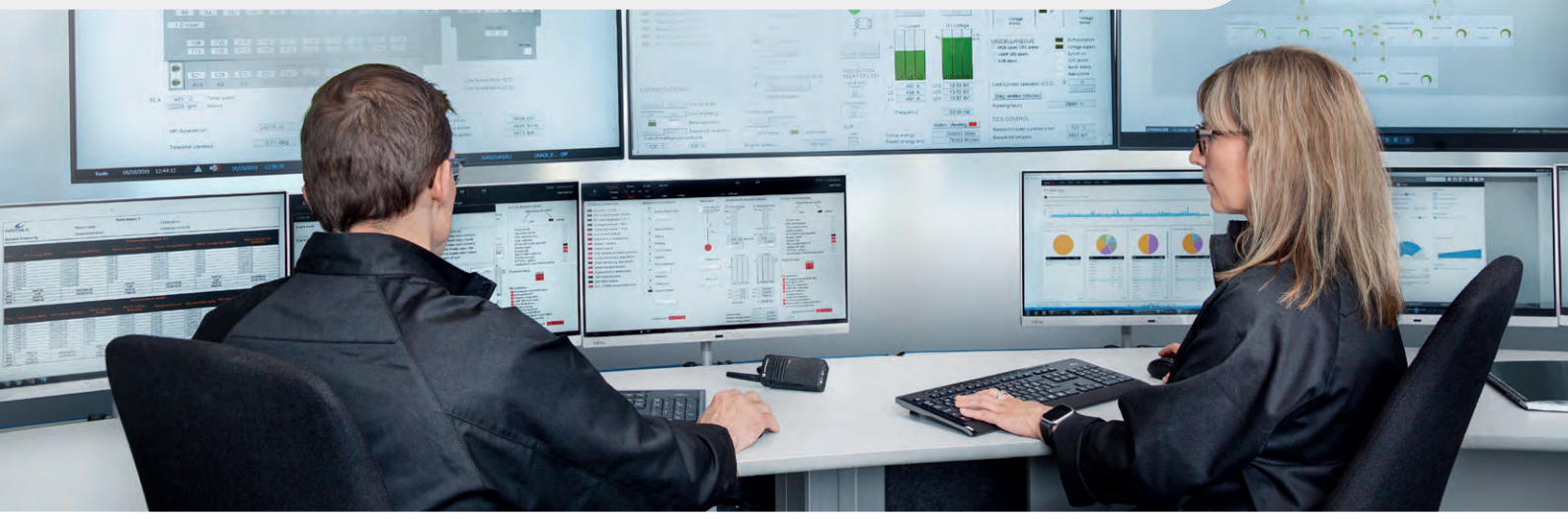
Why choose Wärtsilä?

As an OEM and service provider, we have a thorough understanding of the vessel systems and equipment that require securing. We can provide complete lifecycle support to mitigate cyber security risks along with a wide global service network of skilled service engineers, central cyber security experts and strategic partnerships.

Wärtsilä Cyber services are suitable for all marine installations and ports. Delivery is always tailored according to your specific needs and situation, but we recommend starting with a cyber assessment to define your current situation and identify what steps are needed to effectively mitigate your cyber risks. Our vulnerability management services (Wärtsilä ICS asset visualisation service, Wärtsilä ICS vulnerability advisory service, Wärtsilä ICS patch validation service and Wärtsilä ICS patch deployment service) have been developed as a seamless and cost effective solution for marine installations and ports.

Your benefits

- Identify your cyber security risks and understand the actions needed to mitigate them
- Maintain an auditable and managed program to control your cyber security threats
- Ensure preventative protection of your installation against cyber risks and safeguard products and service operations
- Recover quickly and maintain resilience to ensure maximum operational uptime and availability while increasing the reliability of your industrial control system assets



WÄRTSILÄ® is a registered trademark. Copyright © 2023 Wärtsilä Corporation. Specifications are subject to change without prior notice.