ABS CYBERSAFETY

Cyber threats and attacks are happening around the world. Do you know how to protect your valuable assets? ABS can help.

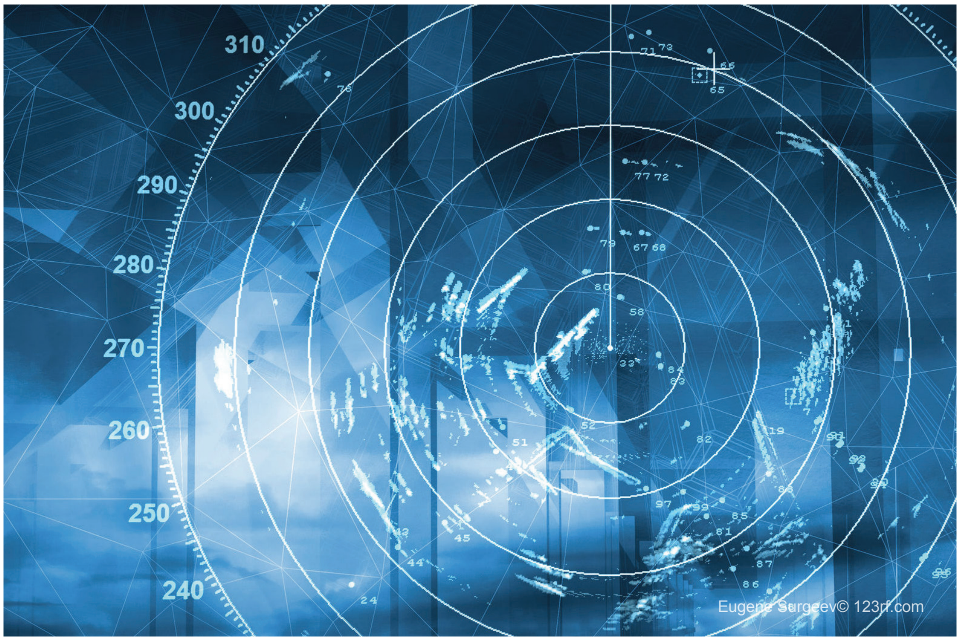
The ABS CyberSafety® team brings decades of multidomain security, cyber and industry-specific experience to developing the first risk-based management program that includes actionable information for improving cyber intelligence and security implementation based on best practices. The ABS CyberSafety program provides asset owners, shipyards, designers, vendors and ship managers with tools and knowledge to understand, manage and help mitigate the risks connected to cybersecurity, software quality and data integrity. Fortunately, most cyber issues are preventable.

The leading cause of cybersecurity breaches are unintentional acts via common points of vulnerability:

- Web browsers
- USB ports
- Wireless routers
- Mobile telephones
- Remotely operated systems and remote access to shipboard components
- Navigation/GPS systems (chart updates)
- Personal devices
- Entertainment systems/WiFi – Internet/Satellite systems

When these common points of vulnerability are breached, critical activities can be compromised, including:

- Propulsion plant control
- Navigation/ship control
- Drilling system control
- Ballast system control
- Crew management



Eugene Sergeev© 123rf.com

The multifaceted ABS CyberSafety program comprises:

- Onboard Operational Technologies (OT) and Information Technologies (IT) assessments
- A review of owner/operator cyber capabilities
- Cyber risk assessments
- Cybersecurity management system assessments
- Verification and validation of software quality engineering practices

CYBERSECURITY

The ABS *Guide for The Implementation of Cybersecurity for Marine and Offshore Operations* provides a model for implementing cybersecurity programs. The ABS *Guidance Notes for the Application of Cybersecurity Principles to Marine and Offshore Operations* describes industry best practices for protecting organizations from cyber threats. Further cyber-specific documents will describe industry best practices for test procedures, automation and autonomy.

ABS issues a Cyber Certificate for compliance with ABS criteria. The notation indicates the level of cyber preparedness of the owners/operators, people, processes, procedures and assets.

CS1 **Informed CyberSafety Implementation**
Informal management of risks, policies and procedures. Informal management of the OT and/or IT cybersecurity threats and technology landscape.

CS2 **Rigorous CyberSafety Implementation**
Formal systematic risk management via global enterprise policies and procedures. The organization is fully resourced to manage the OT and/or IT cybersecurity

threats and technology landscape and can effectively respond to changes in risk.

CS3 **Adaptive CyberSafety Implementation (Highest level of Readiness)** Formal systematic risk management via global enterprise policies and procedures with demonstrable continuous improvement processes. Fully resourced to manage the OT and/or IT cybersecurity threats and technology landscape. Effective proactive responses to changes in risk.

A plus appended to the notation, e.g. CS1+, indicates the shoreside facility complies with the ABS Cyber Guide in addition to the asset.

SOFTWARE QUALITY

A review of software systems increases confidence in software reliability, improves safety, decreases commissioning time and downtime and reduces the risk of software-related incidents.

The software system review assesses compliance with criteria that enhance the robustness of the industrial control software and maximizes the ability to defend against cyber threats.

ABS has developed guidance for software integrity:

- The ABS *Guide for Integrated Software Quality Management (ISQM)* is a risk-based software development and maintenance process built on internationally recognized standards. It helps manage software over the life of the asset
- The ABS *Guide for Software Systems Verification* focuses on Hardware-In-the-Loop (HIL) testing of control system software.
- The ABS *Guidance Notes for Software Provider Conformance Program* provides step-by-step guidance for software houses to implement ISQM for safety-critical systems and equipment.

ABS is committed to cyber safety as part of its mission to promote the security of people and assets and to preserve the natural environment. Contact the ABS CyberSafety team today to address your cybersecurity concerns.

© donvictorio/Shutterstock

ABS

WORLD HEADQUARTERS
16855 Northchase Drive I Houston, TX 77060 USA
P 1-281-877-5800 I **F** 1-281-877-5803
ABS-WorldHQ@eagle.org I www.eagle.org