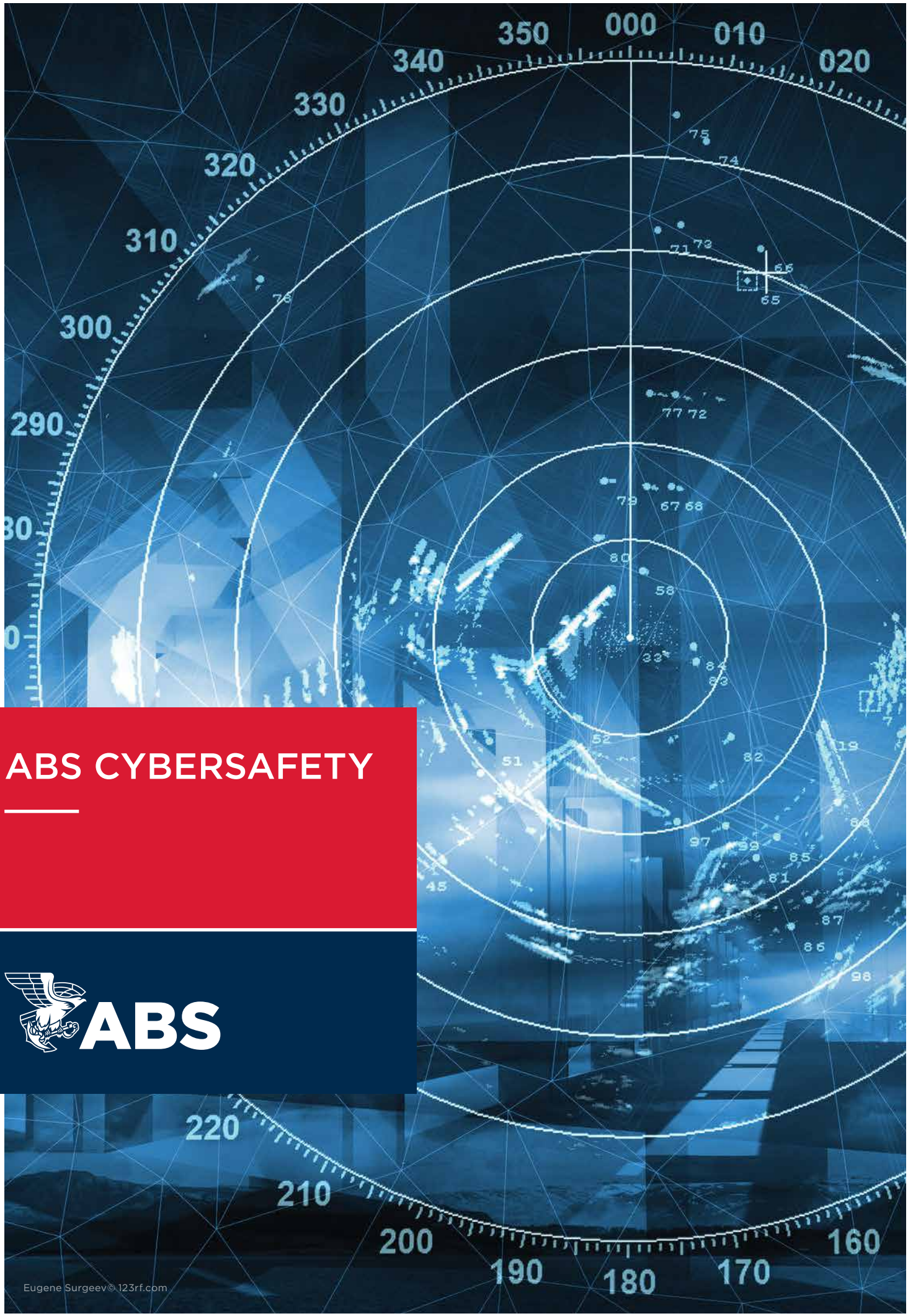
ABS CYBERSAFETY



Eugene Surgeev© 123rf.com

GROW YOUR CYBER INTELLIGENCE TO PROTECT PEOPLE, THE ENVIRONMENT AND ASSETS

The world is full of issues about cyber threats and attacks. No one is immune. Do you know how to protect against your biggest vulnerabilities? ABS can help.

With the **ABS CyberSafety™** program, ship and asset owners, shipyards, designers, vendors and ship managers have the tools and knowledge needed to help mitigate the risks connected to cybersecurity, software quality and data integrity. ABS has compiled an industry standard with actionable items to improve cyber intelligence and security implementation based on best practices.

Most cyber issues are preventable. The leading cause of cybersecurity breaches are from unintentional acts via common points of vulnerability. The most common points of vulnerability include:

- Web browsers
- USB ports
- Wireless routers
- Mobile telephones
- Remotely operated engines/parts
- Navigation/GPS systems (chart updates)
- Crew personal devices
- Entertainment systems/WiFi – Internet/Satellite systems

These common points of vulnerability can be breached at any time affecting your most important activities, including:

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

The ABS CyberSafety program comprises:

- A review of the Operational Technologies (OT) and Information Technologies (IT) onboard an asset.
- A review of owner/operator cyber capabilities.
- An assessment of cyber risks.
- A management system audit.
- A software systems review.

Tests designed to evaluate asset risks may be run and verification will be made for each asset through initial survey on board and annual renewal surveys.

ABS commends its CyberSafety program to owners as a demonstrable commitment to safety in protecting your people, assets and the environment.

The ABS *Guide for The Implementation of Cybersecurity for Marine and Offshore Operations* defines the process. The ABS *Guidance Notes for the Application of Cybersecurity Principles to Marine and Offshore Operations* describes industry best practices in cyber safety used by ABS and other global businesses in protecting their organizations from cyber threats. Further cyber specific documents will describe industry best practices for Test Procedures, Automation and Autonomy.

An ABS Cyber Certificate will be issued for compliance with ABS criteria. A private classification notation can be provided upon request. The notation indicates the level of cyber preparedness of the owners/operators, people, processes, procedures and vessels/assets.

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

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

CS2 **Rigorous Cybersecurity Implementation**
Formal systematic management of risks. Global enterprise policies and procedures implemented. The organization is fully resourced to manage the OT and/or IT cybersecurity threats and technology landscape. Effective responses to changes in risk.

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


© donvictorio/Shutterstock

SOFTWARE SYSTEMS REVIEW

The ABS CyberSafety program may require a software systems review. The benefit to the owner and crew is an increased level of confidence in software reliability with the goals of increasing safety, decreasing commissioning time, decreasing downtime and reducing the risk of software related incidents.

The review is an assessment of compliance with criteria that enhance the robustness of the industrial control software and will maximize capabilities against cyber threats. ABS has compiled several industry standards:

- The *Guidance Notes 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 vessel's life.
- The *Guide for Software Systems Verification* focuses on Hardware-In-the-Loop (HIL) testing of control system software.

Together these standards provide methods to validate the integration of multiple vendors and systems and enable assessment for new construction, modifications, retrofits and upgrades to existing vessels. Industry best practices for Type Approval of related software are detailed in the *Guidance Notes for Software Provider Conformity Program*.

A certificate will be issued for compliance with ABS criteria. A classification notation may be provided upon request:

SQM Nonintegrated control system compliance from design through operation

ISQM Integrated control system compliance from design through operation

SSV Control Systems included in the Verification Plan

DATA INTEGRITY

System and data protection measures contribute to data integrity and reliability and this is especially important for integrated systems (e.g., vehicles) and sensor networks tied to decision aids (Internet of Things).

Safety decisions require secure systems that lend confidence to data integrity. Transmission security, secure storage and quality of service all contribute to the security and value of data. Verification of system security will remove uncertainty in operations, while giving reliability to compliance reports dependent on company data.

ABS has developed the *Guidance Notes on Data Integrity for Marine and Offshore Operations* to help owners and builders alike appreciate this step-change in technology.

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

ABS


© Alex Kolokythas/Shutterstock


© snapinadil/Shutterstock

TX 08/16 16161