ABS
FOUNDED 1862

Cybersecurity

Guidance Notes for the Marine & Offshore Industries

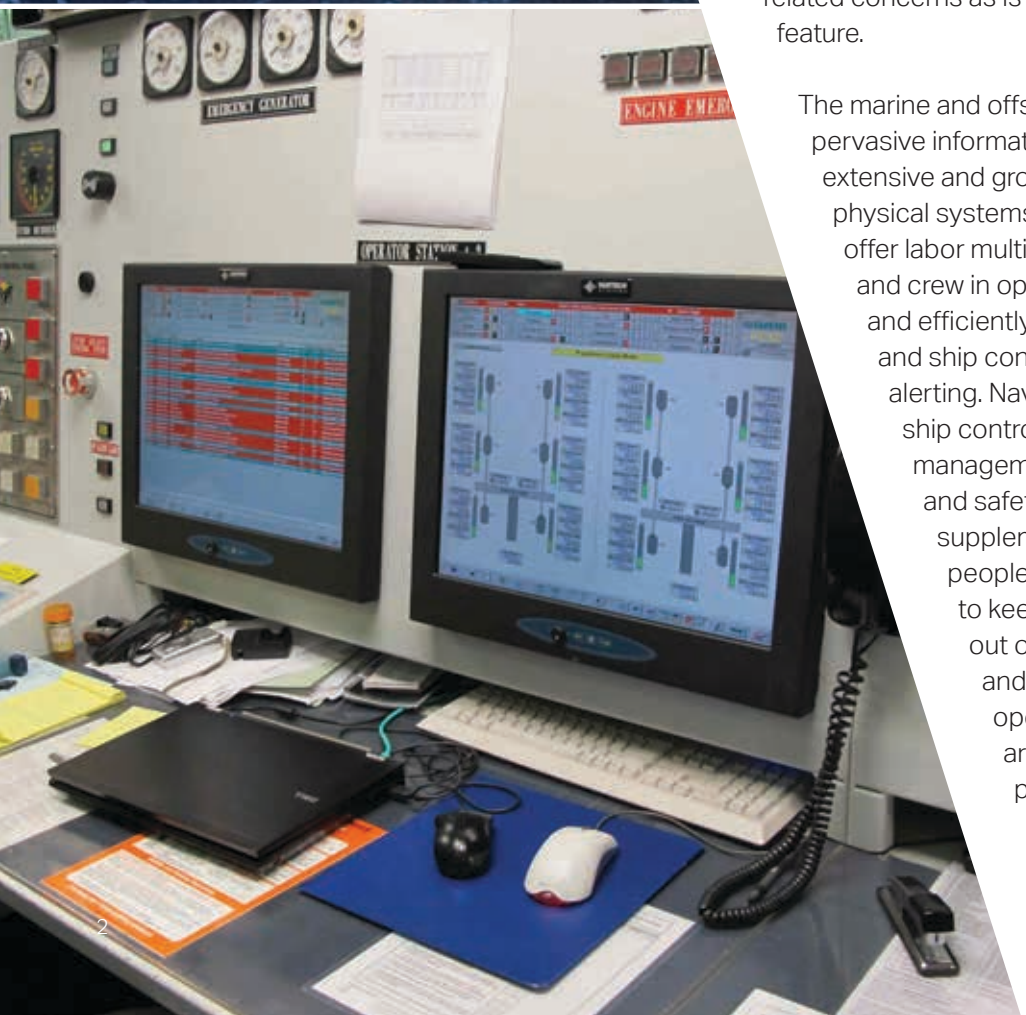
ABS CyberSafety™

Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations is the first volume in the ABS CyberSafety™ series. It provides best practices for cybersecurity as a foundational element of overall safety and security within and across the marine and offshore industries.

The Guidance Notes document leads the new series of ABS publications, which will address both safety and security aspects of cyber-enabled devices, systems and assets. The ABS CyberSafety™ series is the industries' first risk-based management program for asset owners to apply best practice approaches to four key cyber areas: cybersecurity, automated systems safety, data management and software assurance.

Cyber-enabled Systems are Spreading Rapidly

ABS recognizes that automation methods – and increasingly, autonomy – have penetrated nearly all aspects of shipboard and platform systems. Because these systems control multiple aspects of asset, ship or platform operations, they become integral parts of system and operational safety. As such, they also have become subject to the same safety-related concerns as is any other critical vessel feature.



The marine and offshore environments include pervasive information technology (IT), and extensive and growing numbers of cyber-physical systems (CPS). These systems offer labor multipliers to assist the captain and crew in operating the ship effectively and efficiently, providing machinery and ship controls, monitoring and alerting. Navigation, propulsion, ship control (maneuvering), system management, cargo management, and safety sensors and alarms – all supplement people and assist people while providing functions to keep people working and out of harm's way. Both IT and CPS systems must operate as expected if they are to support the crews' processes and procedures.

Ship and platform automated systems are now connected in ways never before considered. Crews, vessel operators, platform or facility managers, and original equipment manufacturers (OEMs) want remote access, greater on-station function, frequent sensor reporting, and new types of data and functions. To support these requirements, many control systems are coupled via industry-standard communications and networking, interfaced to Internet-connected networks, and operated in multiple modes unanticipated at system design. The result is that general-purpose systems are frequently connected to special purpose process control systems, exposing control systems to security incidents that can have operational consequences.

Cybersecurity is the Critical First Part of CyberSafety

Successful cybersecurity is the result of a complex series of related and interdependent work efforts that intersect so as to provide protections that are functional and enduring in the face of challenges presented by geography, technological evolution, and shifting human resource capabilities and deployment.

A thorough understanding of the marine or offshore organization, its supporting physical and intellectual assets, and the needs and capabilities of its people provides the foundation for a structured cybersecurity program. That security program expectedly changes and develops as it orders and prioritizes requirements, builds functional capabilities, and aligns with the organization, its mission and its goals. The organization's IT and CPS systems, and the functions they provide, are the protected assets supported by the maturing security program.

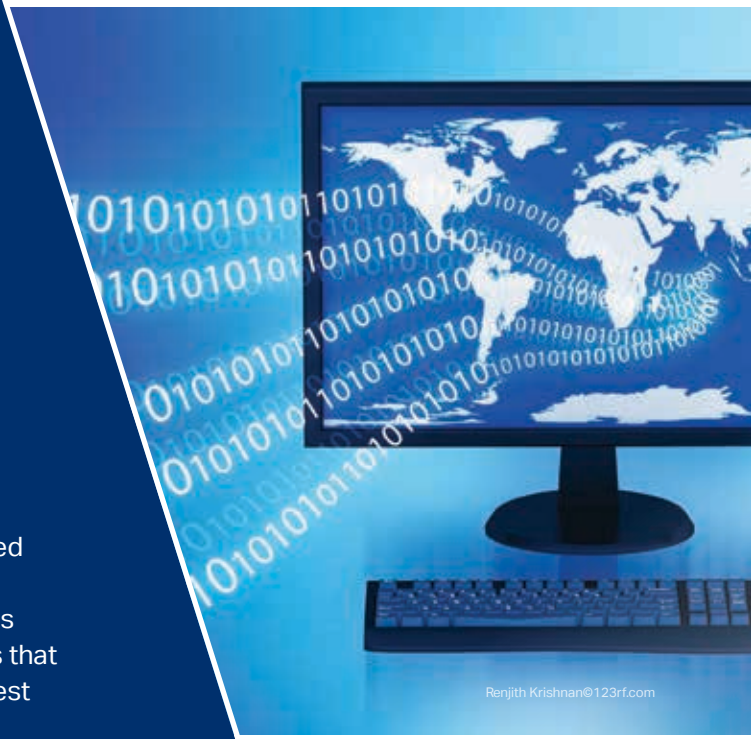
Definitions

CyberSafety

Guidelines and standards for computerized, automated, and autonomous systems that ensure those systems are designed, built, operated, and maintained so as to allow only predictable, repeatable behaviors, especially in those areas of operation or maintenance that can affect human, system, enterprise or environmental safety. CyberSafety is required for the deterministic behaviors found in engineered functional assurance, and it includes software integrity management to manage technical risk in software-intensive systems.

ABS CyberSafety™

Measurable implementation of CyberSafety that tailors cybersecurity and systemic safety to assets in order to enable and encourage risk-based asset management as a systemic outcome. ABS CyberSafety™ will provide deterministic outcomes when implemented within managed environments that include appropriate processes, policies, system test and audit, and data.



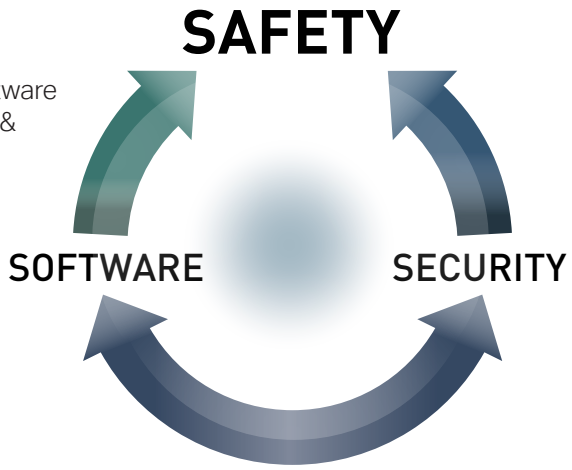
ABS CyberSafety™ is the Risk-based Approach to Cybersecurity

A cybersecurity incident on a ship, on a platform, or within a facility, might result from system fault or failure, operator error or inaction, inadvertent conflicts in incompatible software, or deliberate malfeasance or malice. Any such incident may result in intrusion or malfunction in a general purpose network, resulting in a cascading failure that can spread into ship or platform CPS to cause unexpected consequences for any number of systems.

Because of system interconnections, a CPS failure might even bring about ship-wide failures that can, in turn, affect the surrounding community and environment.

- Critical components
- Automated systems
- Vehicles

- Universal presence
- Critical function software requires verification & validation



- Personnel
- Systems
- Assets
- Processes
- Organizations
- Data Integrity

Auremar©123rf.com

Cybersecurity and software integrity management are both increasingly important to the broader understanding of our systems, our software, and our overall system safety. Cyber-enabled systems and gear are all around us. The security and risk aspects of highly automated, integrated, computerized gear must be well understood in their operational contexts, especially when considering the safety-related impacts of security on both individually controlled systems and linked systems.

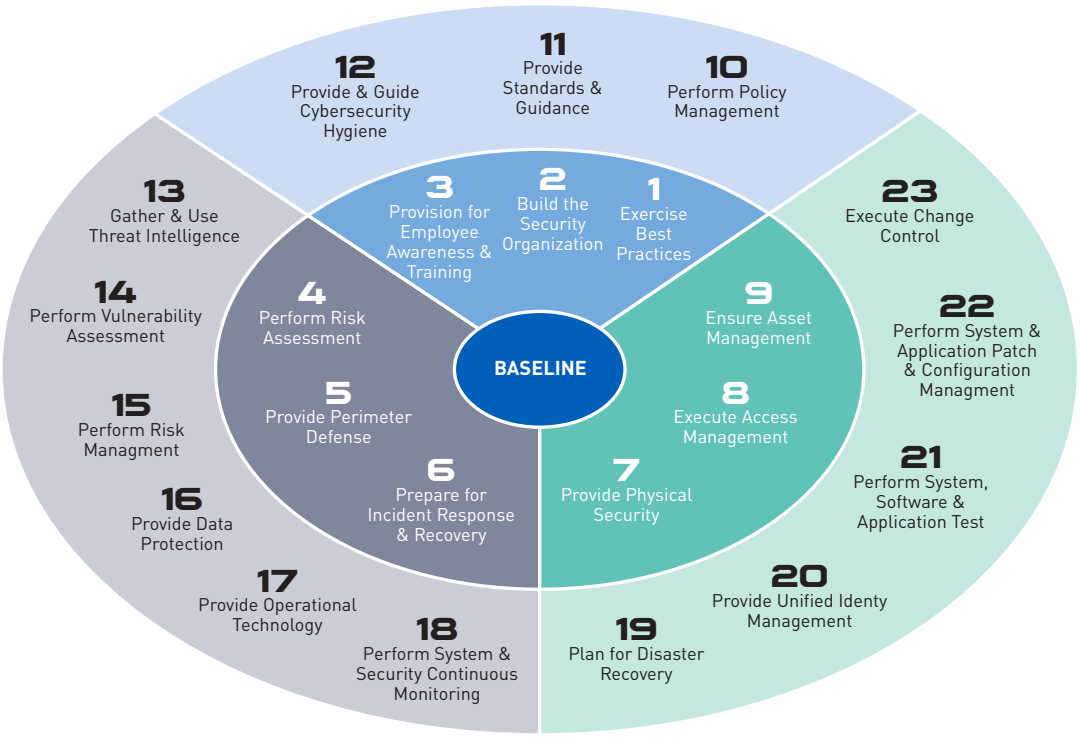
It is with these factors in mind that ABS CyberSafety™ can provide the structure and execution priorities needed by owners, operators and sailors as they safely and securely operate their automated and cyber-enabled systems. The risk-based approach to cybersecurity provided by the method allows measurability and consistency in both processes and controls, thereby contributing to better understanding of systems, personnel, data and security status.

The ABS CyberSafety™ Method

ABS CyberSafety™ is the ABS process for adding cybersecurity rigor to both the operational systems aboard ships and platforms, and to the linked business systems that support their missions. The best practices in these Guidance Notes will help the reader understand how to frame and prioritize cybersecurity work efforts in going about building determinism, security and safety into systems.

Volume 1: Cybersecurity provide best practices in the context of Basic and Developed Capabilities that fully enable a cybersecurity work effort. In this context, a Capability is broad in that it includes people, systems, data, and processes. An organization builds these Capabilities incrementally based on security needs, staff competencies, available acquisition resources, and organizational maturity in cybersecurity.

Capabilities built according to this method become the organization's support framework for security controls, policies and procedures. The program becomes an overlay that can be used with any compliance framework's security controls, or it can be a measurable compliance set in its own right. The arrangement of the Capabilities is consciously structured to provide supportability and life cycle management inside the personnel structures built and maintained by the organization, for both cybersecurity and system safety.



The model illustrates the Capabilities required to build a cyber-safe program that supports cyber-secure systems. At the core of the program are the baseline controls and tasks – the information technology fundamentals – commonly employed to support a business or operational (shipboard, offshore platform or port facility) system. Surrounding this baseline are Capabilities needed to shape an environment that is ready to sustain a robust cybersecurity program.

The nine Basic Capabilities shown should be developed and implemented within the organization, and should be evident as fully documented, employed, supported, and maintained. The more advanced organization will progress to the next fourteen Developed Capabilities, adding breadth and depth to the security program in alignment with organizational priorities and assets. The purpose of this layered approach is that it enables the builder of a cybersecurity program to select and implement Capabilities in a way that best satisfies the needs, constraints, endemic risks and program priorities of the supported organization or asset. In turn, the sustainable, risk-attuned cybersecurity program will better support automation and data gathering, data handling and management, and sensor operations aboard the offshore platform or marine asset. Cybersecurity and CyberSafety are required for data security, to ensure data integrity against system faults and threats, and to give the reliability of data feeding analytic engines. Without security, data integrity from sensors and systems can lack integrity, which may invalidate the data analytics that drive operational availability, maintenance scheduling, and system safety monitoring.

Best Practices

Volume 1: Cybersecurity is organized as best practices and recommendations for each of the Capabilities shown in the preceding cybersecurity program graphic. The Basic Capability list deemed to be essential to a nascent program is provided first, followed by the Developed Capability list.

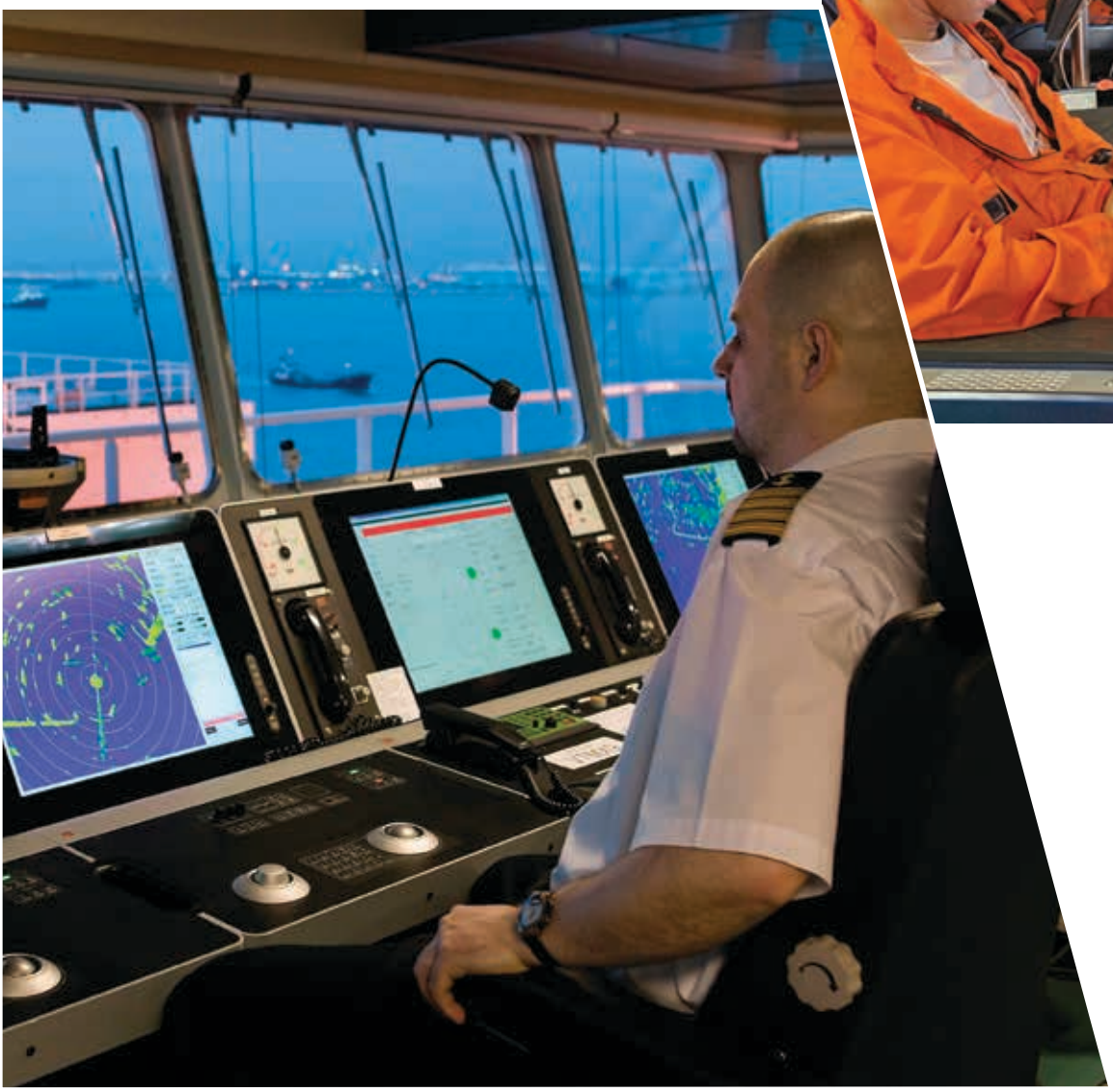
Basic Capability	Developed Capability
Exercise Best Practices	Perform Policy Management
Build the Security Organization	Provide Standards and Governance
Provision for Employee Awareness and Training	Provide and Guide Cybersecurity Hygiene
Perform Risk Assessment	Gather and Use Threat Intelligence
Provide Perimeter Defense	Perform Vulnerability Assessment
Prepare for Incident Response and Recovery	Perform Risk Management
Provide Physical Security	Provide Data Protection
Execute Access Management	Protect Operational Technology (OT)
Ensure Asset Management	Perform System and Security Continuous Monitoring (SCM)
	Plan for Disaster Recovery (DR)
	Provide Unified Identity Management
	Perform System, Software and Application Test
	Perform System and Application Patch and Configuration Management
	Execute Change Control as an Enterprise Process

Not all best practices fit every situation, operational context, or application; even so, the listed practices are primarily based on lessons learned by implementers that have paved the way in cybersecurity program development and can arguably enable a practitioner to stand up a functional cybersecurity program more rapidly and logically than would be possible without this or similar guidance.

Summary

Cybersecurity is the first area to be addressed in building secure and safe systems. As the ABS CyberSafety™ series matures and is implemented by ship and platform owners, operators and crews, additional products will be provided to support self-assessment, self-test, and self-audit of IT, CPS and security programs as a whole.

Volume 1: Cybersecurity addresses cybersecurity practices for systems, ships and platforms as part of the ABS CyberSafety™ series. Beginning with best practices, the series will help owners, operators and regulators to verify the various automated systems found at sea and ashore can neither cause harm to personnel, nor compromise system integrity or operations. Other volumes in series will provide test, data management, software assurance, automated systems (i.e., robotics and safety-critical systems) and autonomous system guidance and technical direction. Appendices to the ABS CyberSafety™ document series will provide strategy, policy, processes, and safety assessment tools, checklists and audit templates.



Watchara Rojjanasain©123rf.com


Goodluz©123rf.com

TX 03716 16053

World Headquarters
16855 Northchase Drive
Houston, TX 77060 USA
Tel: 1-281-877-5800
Fax: 1-281-877-5803
Email: ABS-WorldHQ@eagle.org
www.eagle.org

ABS
FOUNDED 1862