The World's Largest Circulation Marine Industry Publication • The Information Authority for the Global Marine Industry since 1939 • Number 5 Volume 79

MARITIME REPORTER AND ENGINEERING NEWS

MARINELINK.COM

May 2017

The Promise & The Challenge of Maritime's

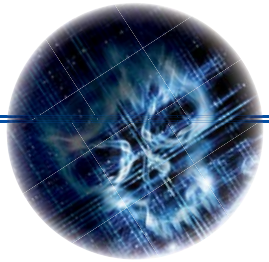
Cyber Future

Sveinung JS Støhle & Hoegh LNG
Banking on Gas

Marine Propulsion
Hybrid Drives are Here

Kaity Arsoniadis-Stein & VIMC
A Maritime Hub Grows

Pockets of Growth
Shipbuilding 2017



Hyper Connectivity: The Risks and Rewards

By John Jorgensen,
Chief Scientist,
ABS CyberSafety

The maritime industry is becoming more connected – at sea, on land and in between. This trend has given rise to a cyber-enabled fleet that continues to adopt greater levels of automation and operational complexity.

For the end user, the benefits of modern shipping are multiple. For the ship owner or operator, however, every incremental advance of technology creates new entry points for risk.

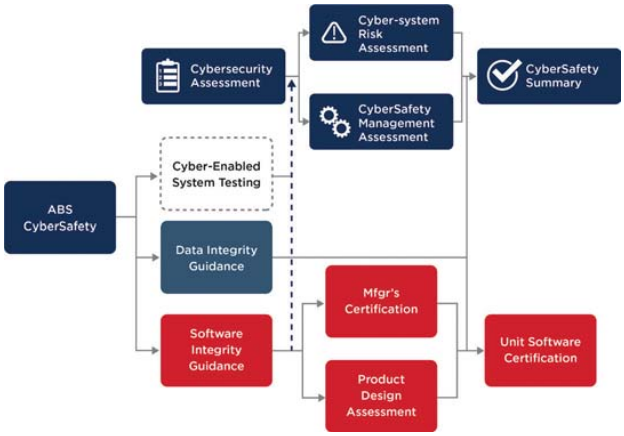
In this hyper-connected era, defending against the introduction of new risks as technology changes demands a recommitment to systems engineering and, more broadly, established risk-engineering techniques to embed processes that maintain cyber-resilience for all stakeholders.

Functional systems on marine assets are specialized to satisfy particular needs, and they are generally built in relative isolation from each other. Propulsion plant control systems, dynamic positioning systems, ballast and emissions control systems, and many other cyber-enabled, software-intensive components enable crews to work efficiently. These systems are often designed and built by separate manufacturers and, when they are installed, their interfaces and connections require integration.

Integrating hardware from varied manufacturers using multiple pieces of software can introduce a broad spectrum of risks, particularly if the process does not take an organization-wide view or follow established engineering and security principles. Adding to the complexity, the cyber-enabled components of control systems often include a mix of Internet Protocol (IP) communications and non-IP communications and protocols.

All this requires integration strategies to be custom built to the asset class and operational environment they are trying to protect. Tailoring helps operators to avoid failures that cascade beyond the individual system or asset into the wider stakeholder community.

The shipping community differs from other industries in that its main assets are designed and produced in short production runs. From a systems perspective, most ships differ from unit to unit, even between sister-vessels. One strategy does not fit all.



There are three fundamental categories of assets and activities that should concern cyber-conscious shipowners and operators:

1. Operational control systems and technology;

2. Information technology and the networking that connects everything (such as public Internet or private intranets); and

3. Human processes (this is the area most frequently neglected).

Integration Consequences

Understanding the operational consequences of integrating onboard systems is a considerable challenge, particularly when information technology and operational technology (OT) systems are combined.

IT-OT systems tend to require continuous upgrades as older software, components and methods are retired or improved. The updates may bring new operating efficiencies for asset owners, but they also offer new opportunities for errors, dysfunction and intrusion.

To maintain cyber resilience, any systems or software upgrade requires a complete reassessment of the organization's risk-engineering processes to determine if any new conditions

Reprinted with Permission from the May 2017 edition of Maritime Reporter & Engineering News - www.marinelink.com

and vulnerabilities have been introduced.

A new risk assessment rebuilds understanding of the operational implications of the new conditions, technologies or methods. As integrated systems become more complex, an organization's methods of risk assessment too require periodic updates to fully understand the consequences of failure for any element in the enlarged network.

When managing change within cyber-enabled OT-IT network it is important to remember two key points: any new condition can introduce vulnerabilities that have a far greater operational impact than intrusion; and failed or corrupted elements do not require a direct functional relationships with safety-critical control systems (or components) to disable them. They simply needs to be connected to that network; risks often inherit upwards from an operating system's least safety-critical component to its most vital.

Both points can be discovered through a new risk assessment, assuming that it includes a human-factor component because change can also introduce human error.

Network Connectivity

Systems – such as those that control a ship's propulsion, navigation, ballast water, power, fire and gas alarms, scheduling and crew management – are frequently connected to ship-wide integrated networks. Any failure of those systems could have safety consequences for the asset and the environment, which puts at risk the wider marine community and the public it serves.

Rigorous systems engineering makes assets more operationally reliable. Understanding the consequences of change is not something that can be deferred in critical systems, or any networks to which they are connected. Established risk-engineering techniques provide the type of systems view helps an owner to understand and manage the factors that impact upon reliability, sustainability and cyber-resilience.

Most methodologies of risk management for technology systems use a tiered approach to determine risk. The U.S. National Institute of Standards and Technology, for example, requires organizations to assess risk in a very basic hierarchical arrangement.

Risks to systems and technology – those that could impact upon systems, machines, applications or data – create the foundational layer of the scheme (see pyramid above). The intermediate level of the model addresses risks to the specific organization's critical processes. Understanding the risks at this level requires a comprehensive knowledge of systems, applications and organizational processes to identify their dependencies; the objective is to understand how a loss of specific systems or data may affect operating and safety-critical processes.

The top level contains the wider risks to the enterprise as a whole, which are informed by the analysis of the risks at the base and intermediate levels.

Back to Basics

The operational risks emerging from an increas¬ingly cyber-enabled, automated marine industry can be managed by broadening established risk methodologies to account for technology-induced variable conditions.

Class societies such as ABS have the foundation in engineering knowledge to help asset owners navigate the 'smart ship' era.

The key to risk-management in a cyber-enabled world is to ensure that knowledge about any asset – including its interdependent systems and components – deepens each time new technology or processes are introduced. There are several ways to accomplish this, but it's probably most instructive to examine the one with which I am most familiar.

ABS CyberSafety

The ABS CyberSafety framework, highlights the most effective engineering and risk-management tools for cyber-enabled and automated systems. It encourages companies and organizations to develop knowledge about their systems while also building personnel and organizational maturity.

The methods are measurable, and they scale to the size of the organization in ways that identify risk profiles across assets, systems and people.

The program includes cyber security and the software and data integrity of each of the owner's assets, and it scales to the fleet to manage risk across a global IT infrastructure.

Rapid technological change, heightened connectivity and automation create a complex risk environment. For operational technology, rigorous engineering and assessment are required with each incremental advance of technology. In that environment, assess-ments must be structured to discover whether an asset is operating at risk levels that allow it to remain reliable.

A notional view of the ABS CyberSafety assessment process, encompassing the engineering and risk-assessment activities, is below.

The broader process, showing the major components of the framework, includes cyber security, data integrity, software integrity and cyber-system testing (under development). The breakout portion of the diagram shows an assessment that starts with the security of cyber-enabled systems, including the organizational factors such as policies, procedures and processes. Subsequent stages add risk and management assessments, and the process completes with a summary report of risk conditions, system gaps and recommendations for priority actions.

As marine systems and assets become more complex and connected, a renewed dedication to established systems and risk engineering will help to manage the process of technological change, while keeping the safety of your people, assets and the environment at the forefront.