Managing Human Cyber Risks in the Maritime Industry

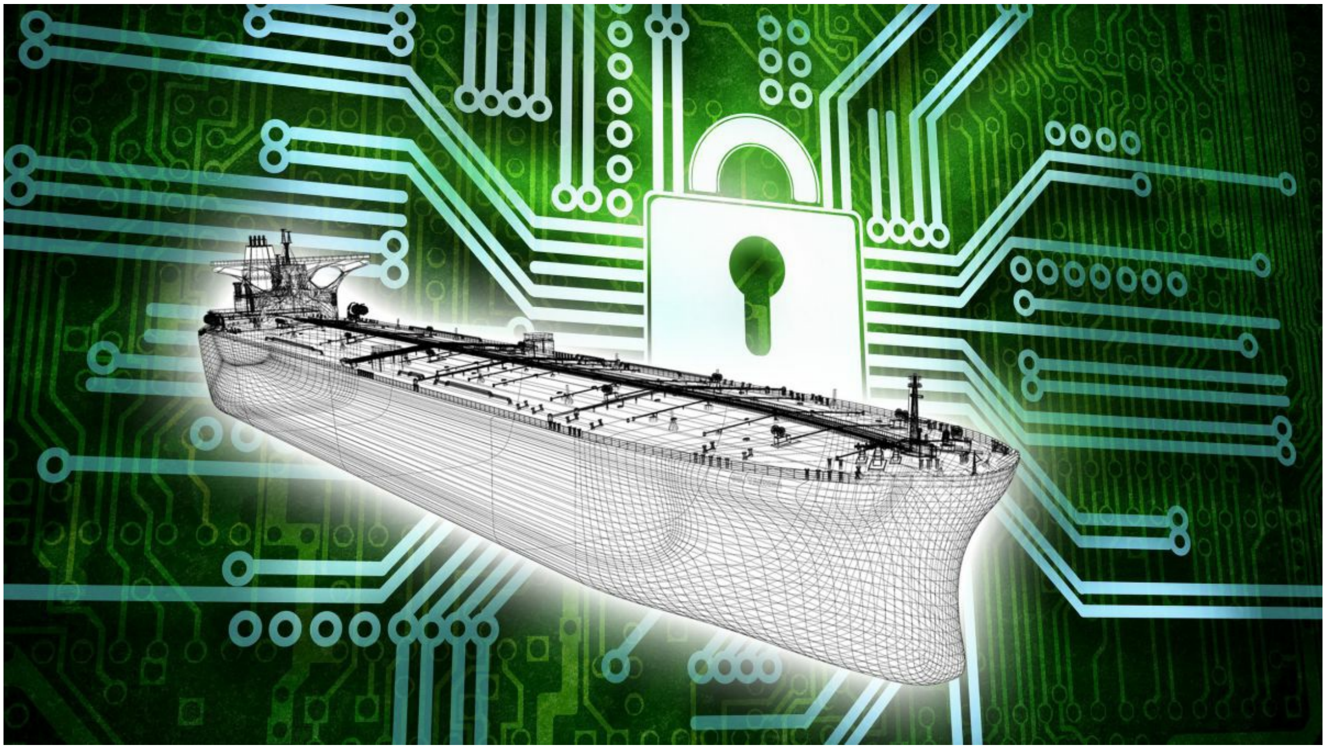


Image courtesy ABS

By **John Jorgensen and Kevin McSweeney** 2017-09-08 19:20:55

The pace at which smart ships are being introduced onto the world's oceans is escalating, driven by automation's potential to improve operating efficiency and safety throughout the lifecycle of those assets.

While automation is an attractive proposition for ship-owners, it also brings complexity because its introduction requires more than the simple replacement of the functions of older systems. Modern functionality requires systems integration and interoperability with their hosts, which can add unexpected levels of connectivity and new risk factors to the ship or system into which they are integrated.

Every functional advance – even those brought about by routine software upgrades – introduces new entry points for systems intrusion and new potential for operational failure. Even though automation is increasingly about controlling risk and complexity, building cyber resilience is not only a technical challenge: it is a personnel challenge.

Why? Because employees are the first line of defense against digital risks; but they are also the predominant cause. Their neglectful and malicious acts — including lost laptops, the accidental disclosure of information, and the actions of rogue employees — cause two-thirds of cyber breaches, recent insurance claims data has revealed.

The key to effective systems-risk assessment and management – digital or otherwise – lies in building human understanding of how those systems work. It is a challenge that largely can be met by combining current methods of both industrial and human engineering.

It is important to recognize that more operational complexity (e.g., in systems architecture, rules, policies, procedures, etc.) tends to decrease an individual's situational awareness and increase the likelihood of human error.

So, as systems gain complexity, efforts to reduce the potential for human error need to be redoubled. This can be achieved through the design and arrangement of a system, for example, by building computer stations without USB ports or by creating closed systems that are unconnected, or isolated by ‘air gaps’ that have monitored and integrated security.

Workforce risks can also be mitigated by strengthening policies that limit access to specific systems, segregating networks, filtering emails and installing browser blocks.

The creation (and constant update) of policy and procedures to support those goals is a tenet of human-factors engineering. Building cyber awareness in the workforce requires a management system that offers a detailed, company-specific roadmap to resilience, including guidelines to manage change.

Once the corporate plan is created/revised, employees need the skills to deliver it; and like the policy and procedures, those skills must be constantly updated to reflect the evolving nature of the risk. As the commercial environment becomes more techno-dependent, security training – especially initiatives that encourage the right attitudes and behaviors – becomes more critical. The provision of training is simply not enough. Competencies need to be continuously demonstrated and validated. Cyber awareness itself needs to become a critical behavior.

From an engineering perspective, the integration of systems makes sense; modern systems are built to encourage the consolidation of functions. Their builders incorporate network links where it makes sense for systems to use connectivity and provide interoperability. It is part of automation’s attraction.

However, inter-system connections can introduce unanticipated communications paths, which complicates matters on many levels, from systems security to employee training.

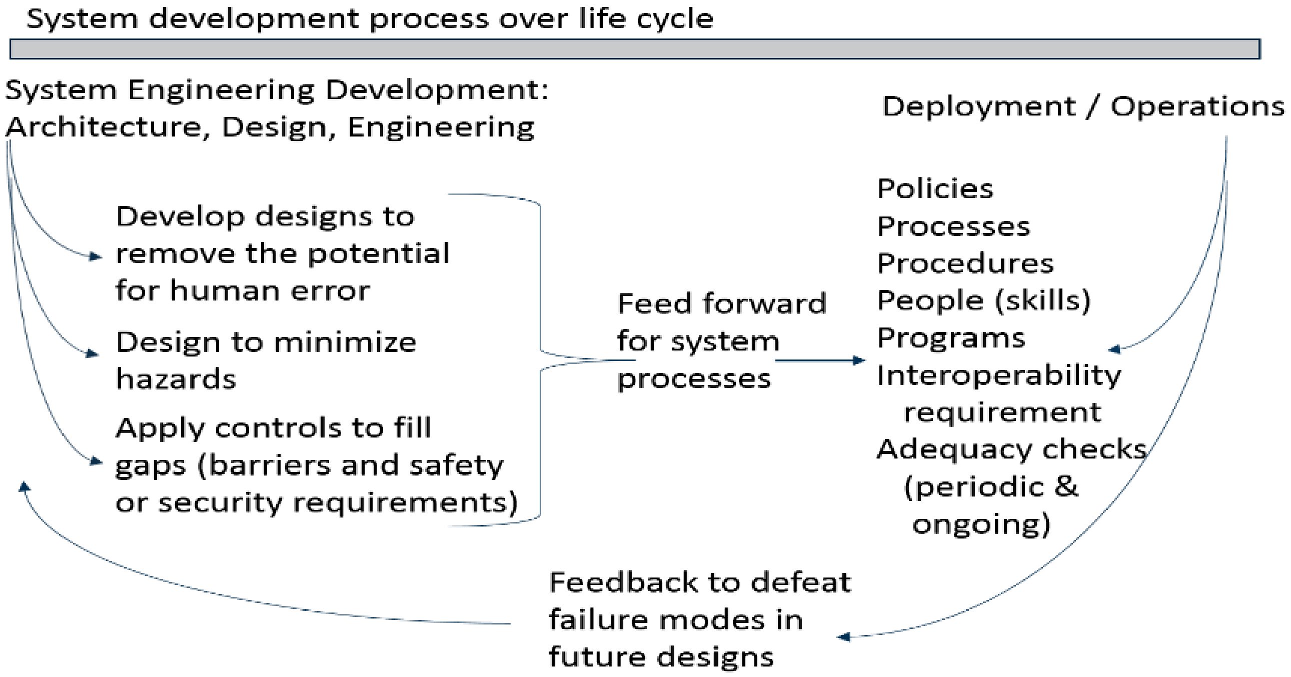
Crews and operators are trained according to the methods and functions for which systems are originally designed and built. The characteristics and performances of individual systems are largely documented by their designers; understanding the behavior of systems that are connected, integrated and/or interdependent is more complex. The potential for disruption often multiplies beyond the sum of the parts.

Systems of systems, such as those increasingly found on modern marine assets, increasingly use networking to connect IT systems and operational technology (OT) systems.

The greater the complexity, the less likely it is that all operating or risk conditions have been recognized, documented and tested. On one hand, greater demands for operational efficiency and system economics compels builders to integrate systems; on the other, crews need to understand their operating environment, failure modes and resilience characteristics to secure the systems, their users, the ships and the natural environments in which they operate.

That creates a conundrum: how do shipowners assure the operational efficiency, security and safety of their assets and systems while addressing the risks brought by the complexity of an increasingly connected world? Systems do not simply snap together like a child’s building blocks; but there may be an understandable answer at both ends of the asset lifecycle.

The process of systems engineering starts by developing the concept and analyzing its requirements. Its functional requirements – the end-user needs, or why it is being built -- combine with non-functional requirements, including performance, human factors, data integration and security, etc. (They are later expanded to include extra-functional requirements such as resilience and security-process support.)


System development process over life cycle
System Engineering Development: Architecture, Design, Engineering
Deployment / Operations
Develop designs to remove the potential for human error
Design to minimize hazards
Apply controls to fill gaps (barriers and safety or security requirements)
Feed forward for system processes
Policies
Processes
Procedures
People (skills)
Programs
Interoperability requirement
Adequacy checks (periodic & ongoing)
Feedback to defeat failure modes in future designs

On the left side of the engineering lifecycle timeline (*above*), architecture and design processes shape the system to reduce the potential for errors, malfunctions, safety hazards and security vulnerabilities. The extra-functional requirements for security and safety include the engineering of the human/computer interface as part of the design.

On the right side are the deployment, operations and maintenance phases, where the operators integrate with the systems and where associated knowledge and understanding work to their advantage.

Corporate knowledge, including operator and service manuals, test processes and results, failure modes and indicators, as well as incident or anomaly recognition and response procedures, are all documented and maintained in a functional description document. This document hosts information about the system architecture, design, an as-built diagram, test results and any other system-related information that needs to be understood as well as the associated training.

Developing an organizational cyber culture is similar to developing a safety culture in that a well-defined structure will help to engineer risks – human or industrial -- down to acceptable levels. Designing and implementing organizational values, attitudes, perceptions, competencies and patterns of behavior may appear to lend themselves less to structured development than, say, building skillsets, but they are just as foundational to cyber resilience and the implementation of any program.

From a human engineering perspective, the basics of a healthy organizational cyber culture will include (but not be limited to):

- *Company-specific programs that build an understanding of cyber risks*
- *Strategies for employee engagement (to build knowledge and situational awareness, and to avoid complacency)*
- *The creation of a just culture in which workers are seen to be treated fairly (this is different than a no-blame culture in that it includes worker accountability)*
- *A commitment to employee empowerment (to help them fulfill their responsibilities)*
- *The promotion of personal integrity (so employees do the right thing, even when no one is looking)*

- *A visible commitment to cyber resilience from the corporate leadership*
- *Effective communication practices (including positive and negative feedback)*

Policies, procedures and training should be viewed as management-system barriers designed to prevent or limit the scale of undesired events. But those barriers cannot be erected and then forgotten: their health needs to be measured and modified as systems and risks evolve.

Decades of dedication to building maritime safety awareness has provided us with the human and industrial engineering practices and methodologies that are now required to build cyber resilience across an increasingly connected modern systems architecture.

As systems become more complex, connected and cyber-enabled, many solutions to the emerging risks can be found in what we already know.

John Jorgensen is Chief Scientist and Director of Cyber Security. Kevin McSweeney is Manager, Advanced Technology & Research - Human Factors, Safety, and Emerging Inspection Technology. Both work for ABS.

The opinions expressed herein are the author's and not necessarily those of The Maritime Executive.

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.