CLASSIFICATION CONSIDERATIONS FOR CYBER SAFETY AND SECURITY IN THE SMART SHIP ERA

G Reilly and **J Jorgensen,** American Bureau of Shipping (ABS)

SUMMARY

As the marine industry develops and introduces new technologies, it is the purview of Class societies to consider the potential impacts of those technologies on safety. Further, Class societies develop guidance and rules that embrace the benefits of evolving technologies while assessing the risks associated with their use.

As the industry has developed more highly instrumented, automated and interconnected "Smart" ships, unforeseen technical problems and risks have emerged in ***parallel*** with those developments. The potential for those dangers to be realized increases significantly with the ready ability to connect shipboard equipment and systems to shore. This subject is now familiar to the public as "Cybersecurity." Other industries are arguably farther down the path of integrated and interconnected systems than the marine industry. Therefore, as the marine industry enters the "Smart Era," it is possible and responsible to learn from previous mistakes and to apply the lessons learned, particularly during system architecture design.

Through IACS, Class societies have already started reviewing problems of the complexity in highly interconnected systems, and have recognized that a limited number of cyber related problems result from malicious actions. Poor access protocols, weak passwords, poorly executed updates or modifications and the poor cyber habits of personnel all contribute to cyber problems and need to be addressed. Developing appropriate requirements and tools to take account of the whole system are needed. This paper provides perspective for the various risks that accompany Smart Ships, and it outlines the ways in which Class is maintaining its focus on safety throughout this "Smart Era."

1. INTRODUCTION

System, process and function automation is accelerating across our world as computational power increases, computational costs decrease, and familiarity with inexpensive computational equipment expands through society. Many industries have adopted automation methods, witnessed increases in industrial plant automation methods and in home automation gadgets, and the marine industry is now beginning this transitional journey.

Simple process or system automation leads to programmable methods for automating functions, whether in homes, vehicles, or ships. For marine applications, this gives rise to the concept of a "smart ship," denoting a ship in which personnel strength and intelligence are now augmented with programmable automation functions and labor-saving devices that multiply the crew's ship handling capabilities. It also means more operational functions are possible, with fewer required crew, subject to compliance with international manning requirements.

We will set the stage with definitions for the following discussion.

- Smart Ship: A marine asset built with significant automation in systems, system monitoring and management, and data communications. Automation provides labor-saving methods; human augmentation and error-checking; multiple simultaneous system control and management; and data reporting to enable better and faster decisions. A Smart Ship may have entirely automated, or even autonomous, processes that operate without significant human intervention.

- Cyber-enabled system: A computerized, automated or autonomous system that contains logic, data processing hardware, behavior-governing software, and external communications capabilities. A completely cyber-enabled system may have human-independent communications and behaviors within programmed boundaries that can be addressed or adjusted by external control methods or paths.

Marine Class Societies (to be referred to simply as Class in this paper) perform development and verification of standards for the design, construction and operational maintenance of marine and offshore assets. As third-party technical review organizations Class must track, monitor and maintain currency with the technologies, processes and methods used in marine applications. This helps ensure that Class remains at the forefront of asset, system and process safety. This paper addresses some of the issues seen by Class Societies with the benefit of decades of experience and overall 'horizon views' with the marine industry.

2. PERSPECTIVE FROM CLASS I: LIFECYLE AND TIME FRAME

From the perspective of Class the two dominant phases of the lifecycle of a vessel are construction and operation.

- Construction is dependent on the shipyard and Class engineering approval and survey of best practices, lessons learned and construction standards.

- Operation is dependent on the ship's crew and Class survey of operational best practices, safety and compliance standards.

Until very recently most vessels would operate their entire working lives with only the safety features that were installed at new construction [1]. Ships and seagoing platforms, as mechanical systems, performed certain sets of functions that could be regulated and monitored by crews, who possessed complete knowledge of the systems and their utility or interactions. Safety methods, guarding devices and assessments have been well established in international custom and law [2].

The historically slow pace of change and technology advancement in marine application is changing as automation methods become practical and cost effective for ship and platform owners. As hull, mechanical and electrical (HM&E) standards for mechanical systems are supplemented with automation mechanisms, the functional capabilities of their host marine asset transform into complex, interactive systems of systems that might be called hull, mechanical, electrical, computers and sensors (HMEC&S).

Figure 1 shows a notional view of an ordinary ship requirements cycle [3]. Requirements peak at construction, sharply declining as the ship is delivered, shaken down, and put into service. Requirements for modifications, updates, compliance needs and new systems accumulate until the first (or next, in case of existing ships) five-year overhaul and drydock period. Docking and overhaul work packages will satisfy many of the outstanding modification and update requirements, though probably not all. Cost, perceived relative return, and owner readiness to support such modifications all work toward the balance for whether all requirements are satisfied, or not. The next cycle begins as the ship is placed back in service, and requirements again accumulate until the next major work period. The notional diagram hints at the typical drawing-out of requirements satisfaction towards the end of the asset lifecycle, as fewer modifications or updates in excess of the Class minimums are purchased later in the ship's effective life.

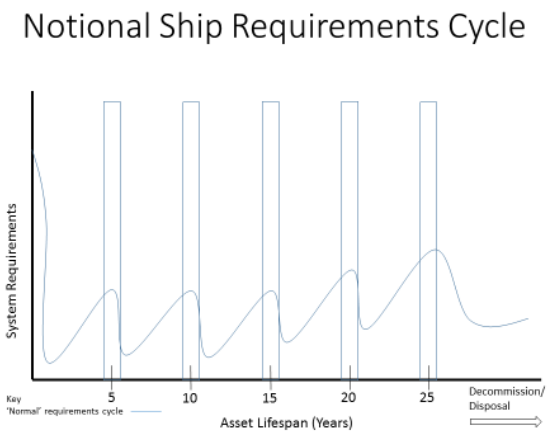

Figure 1: Lifecycle requirements for a vessel were about 20 - 30 years

Over the past 20 years the lifecycle requirement and system configuration stability has remained broadly the same, except that many elements of ship equipment now have shorter timelines for modifications and updates. Integration of greater automation has brought programmable systems and software, both of which may give ships, platforms and crews much greater capabilities. Shipboard software-intensive systems generally break down to include two categories: management systems and operational systems.

Management systems include office automation, general purpose computational systems, and resource management software or systems. Generally networked, these service applications are seldom mission-critical, and they commonly do not, by design, connect to systems that provide control functions to mission systems. This type of software application is updated on a periodic basis, depending on usage and licensing. System updates might force changes in hardware – networks, computers, data storage devices, and processing needs – and the lifecycle of management applications might be as little as a year, but no more than 5-7 years.

Operational systems are software-intensive systems that include cyber-physical systems, i.e., systems that execute control actions on the basis of program code, physical interface devices, and human interface displays, often running free of significant human intervention or action. These systems are part of the basic equipage for modern ships, substituting automation for human attention, and providing control capabilities that transform crews' abilities to operate their vessels. The software for operational systems tends to be longer-lived than management systems, as it provides functions integral to the operation and operational characteristics of the host vessel or platform.

Typical ship or platform requirements now must include the software functions and considerations associated with software-intensive systems. Lifecycle requirements, once largely stable based on finite numbers of possible

improvements or replacements to HM&E gear resulting from long technology evolution cycles, now must include software updates and system upgrades.

Recent history instructs that the lifecycle of typical management system software is 5 - 7 years. Operational system software is often on a longer update cycle, based on multiple factors such as difficulty of updating; difficulty in customers' pre-installation testing; obscurity and/or remoteness of systems; and a 'don't change what works' preference of operational personnel. Based on cost expectations, members of the marine community commonly seek rapid and recognizable value in return for software updates because they are rarely associated with physical construction or drydocking. This lack of recognition of value can directly result in operational systems not being updated, especially if updates are out of sync with asset maintenance cycles, or if costs are required at unexpected times in an asset's lifecycle.

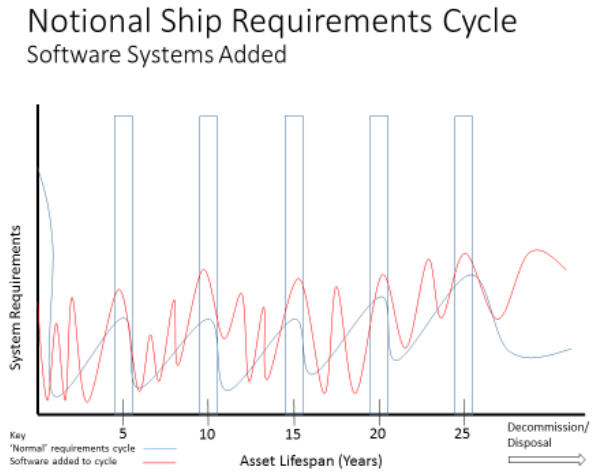

Figure 2: Vessel lifecycle requirements become much less regular with addition of software-intensive systems to the ship's equipment.

With the advent of Smart Ships significant rethinking of these assumptions is needed in several dimensions.

First, software is not commonly associated with only one function or component; instead, it often supports or communicates with interconnected systems. Software can have a disproportionate impact on satisfactory ship operation because of its complexity and influence on multiple connected systems. When these complex interactions are not adequately understood and resulting action unanticipated, satisfactory operation and adequate safeguards cannot be achieved or implemented. This complexity, with its unintended and unforeseen consequences, is at the root of many of the problems that are discovered following software updates.

Second, criticality of software to the functional performance of Smart Ships becomes a significant consideration to overall operational safety. Smart Ships are realized based on the connectivity between components and sensors on the vessel, and the connectivity between the vessel and shore sites that monitor sensors and communicating vessel performance. Security vulnerabilities created by software connectivity may be acceptable in a long-duration update cycle if exploitation of that vulnerability is acceptably unlikely. However, if that software connectivity exposes an operational control system to a known, exploitable vulnerability, then it should be treated as a cybersecurity issue that the owner and operator must address.

Cybersecurity becomes a serious issue for both conventional and Smart Ships because of growing dependence on software for ship control, increases in control system integration, and increases in control system connectivity to onshore monitoring systems. Cybersecurity's effect multiplies because complexity can negatively impact or defeat even rigorous system engineering, due to several factors.

- The multiplicity of cyber-enabled (i.e., computer-enabled or controlled) systems, each of which possesses multiple operating modes or characteristics, can overwhelm designers and engineers, who must accommodate network data flows, continuous power, and connectivity needs as well as the more standard physical installation requirements. This condition can also result in the suboptimization of feature sets for large scale, highly integrated systems.

- Many original equipment manufacturers (OEM) extract and maintain operating data stream reports for their cyber-enabled equipment in order to provide value-added services (e.g., predictive or just-in-time maintenance). OEMs also can and do link warranties with system installation and maintenance conditions, which in turn prevent operators from monitoring data flows or system performance conditions, especially in supervisory control and data acquisition (SCADA) systems.

- Cyber-enabled systems can and do have modes and characteristics that are unknown, and therefore undocumented and untestable, because their communications and performance conditions are considered to be proprietary to the OEMs. When these undocumented features are exposed to external (off-vessel) communications, vulnerabilities in networked connections may be exposed.

- Standardized communications protocols have become so prevalent that communications with individual components, modules or systems may be enabled by default, not by intention. The consequence may be that critical systems, such as main engines, system controls, air compressors, etc., are enabled for outside communications, nominally with their OEMs but unintentionally with security

threats, without the owner's explicit knowledge or permission.

The reality of automation growth is that multiplying interconnections come at a time of increased hazard, whether through malicious code, malevolence of action, or imprudent care and maintenance. Automated and cyber-enabled systems can introduce vulnerabilities that must be assessed for relevance and impact, scheduled and patched, and then tested for residual risk. Combined with expanding communications paths, vulnerabilities can become exploitable weaknesses, thereby making configuration management, patch management and system testing into even more urgent needs within the ship or platform requirements cycle. Figure 3 shows how a security update requirement, when added to previously explored requirements cycles, substantially shrinks reaction times and complicates activities needed to address vessel requirements.

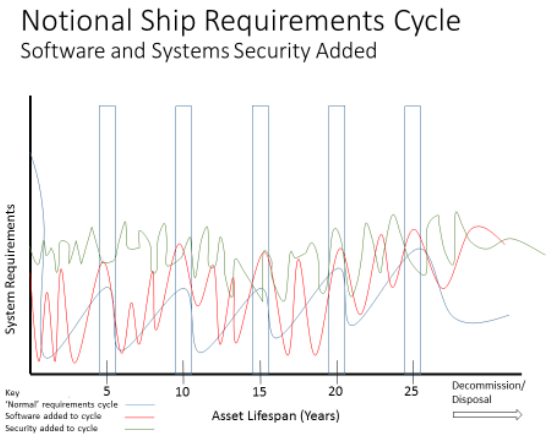

Figure 3: Vessel lifecycle requirements for software protection updates can be far shorter than previous cycles, measuring in days or weeks rather than in months and years.

While the two dominant phases of the lifecycle of a vessel will continue to be construction and operation, it will no longer be possible to use the simple model of:

Construction = Shipyard + Traditional Class Services
Operation = Crew + Traditional Class Services

The crew will have less knowledge and understanding of changes being made by the owner or the equipment manufacturers. The usual, direct and comprehensible ways of alerting the crew of equipment malfunctions or developing problems must transform into more comprehensive and information-rich reporting and action prompts that serve the needs of integrated systems. Software protection methods, coupled with protective architectures, will be deployed to keep operations uninfected and unaffected by unintended communications, but even these will not work against shortcomings in original design architecture or in validating system modifications. The overall process changes will be more rigorous, by including the architecture and engineering processes and capturing knowledge of and about systems and vessels, which will help to ensure all parties involved in vessel life cycle management are informed and involved.

As the marine industry continues to automate assets, there will be a greater pressure on OEMs and shipyards to design ship or platform systems in which the overall system architecture is well defined, documented and communicated so that informed decisions can be made before and during modifications. Better architecture and system engineering should mean that the vessel is delivered with a documented process in place to easily and securely permit security updates. In periodic survey, Class in the Smart Ship future must be satisfied that:

- Systems available on delivery to the shipyard are adequate.
- Systems are followed through delivery to installation and checkout.
- Sufficient system design information is available to enable lifecycle updates in intelligent, informed actions.
- Sufficient processes are in place, followed and documented as evidence that informed actions characterize all critical lifecycle updates.

3. PERSPECTIVE FROM CLASS II: ESTABLISHING A COMMON MEANS OF ASSESSMENT

The purposes of the familiar SOLAS and Class-type requirements are fairly easy to comprehend, even if their intent is not always readily apparent or well explained. The fundamental purpose of marine industry standards is measurably to increase safety in operations and asset use.

For ABS, the overall objectives of Class activities in engineering and survey (*human safety, system or asset safety, and safety for the environment*) remain the same, irrespective of the nature or source of the risk, across assets and throughout lifecycles. Completely external or alien threats could be dealt with directly with appropriate countermeasures, but the risks associated with cyber-enabled systems and Smart Ships are, by their very nature, highly integrated with the vessel's equipment, operation and safety processes. This means solutions that provide good and consistent outcomes must be made available to help surveyors and engineers assess both familiar equipment and the new "smart" systems simultaneously.

As discussed above, traditional requirements, and thus risks, associated with HM&E are generally observable, fairly comprehensible, and have a development half-life on the order of decades. The technology associated with

computer-based systems has a half-life of less than five years [4] and the half-life of the risks can be days or less. Some of the risks are straightforward, but many of them are highly technical and invisible, and frequently embedded by engineers and software developers with limited marine industry domain knowledge.

For Class to be confident that it is continuing to fulfill its mission into and through the Smart Era, it is necessary to bring the different risks and countermeasures into a modified engineering, survey and audit framework that will grow from covering HM&E into an evolved HMEC&S framework. The engineering processes in a new conceptual framework must be familiar to anyone in the marine industry, but these processes will be expanded to include the new factors introduced by cyber-enabled systems.

System engineering processes that will provide useful information and evolving contextual content through an asset's lifecycle include the following.

- Requirements Management: rigorous acquisition methods, approval and documentation of system design requirements; documented update requirements with impact analyses; warm and cold stacking requirements to ensure that no latent obsolescence or cybersecurity risks are present. Requirements Management provides input to all stages of the engineering cycle.

- System Architecture: integration of cybersecurity and cyber-enabled system modes and functions, through related but new documentation, will provide the foundation for system of system understanding throughout an asset's lifecycle.

- Criticality Analysis (CA): mission-critical function and component identification, conducted after design, identifies and prioritizes functions and dependencies that could affect overall system performance or safety. Includes hardware, firmware and software as components of interest for failure modes that could affect system outcomes.

- Failure Modes and Effects Analysis (FMEA): identifies potential failure modes based on failure logic, analysis of dependencies, and outcomes expected from component or system failures.

- Layers of Protection Analysis (LoPA): functional analysis process that uses fault and failure modes as part of hazard analysis, showing where mitigations and countermeasures are required to prevent system failures. LoPA includes cyber protections as part of the functional analysis of systems.

- Software Integrity Analysis: process to minimize software-related risk throughout the life of an asset by analyzing operational software, providing functional verification and integration validation.

- System Test: verifies system functions, and validates user requirements according to stated needs. Ensures performance and behavior meet specified parameters, with specific criteria for suitability to purpose, acceptability for use, and safety in use. Often requires multiple stages (developmental, operational, software, hardware) to provide required evidence for suitability and acceptability.

- Bowtie Analysis: risk analysis method to unify previous hazard, failure and critical dependency analyses in a graphical display, showing causal relationships. Bowtie analysis, in combination with the other analytical techniques, will provide an understandable risk position for the asset and its systems.

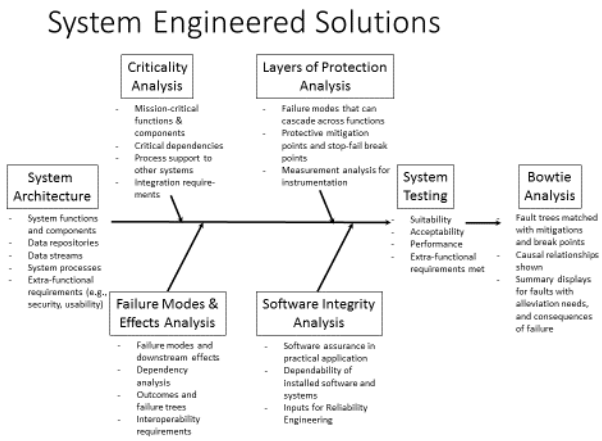

Figure 4: Standard system engineering processes, tuned and phased to provide complementary inputs to the next stages, can provide coverage of new fault types and threat vectors (e.g., cyber) while providing rigor and analytic completeness in the process.

Class engineers and surveyors will review the submissions that have used these analysis techniques to examine relative hazards, failure modes and risks associated with both conventional and cyber-enabled systems, using the processes and methods in a phased and ordered approach to provide insights not otherwise available in standard surveys or engineering examinations. The methods are applicable to engineering outcomes, to which cyber is one of many potential inputs; an experienced Class practitioner in engineering analysis methods will be able to include cyber as another causative function, not as an outcome in and of itself. All the above methods are necessary to ensure Smart Ships can meet their potential; the questions 'what could go wrong *if*...' and 'what outcomes could occur if the following factors go wrong…' are essential to understanding the implications of Smart Ship in the

marine industry, port communities, and regulating Flag States.

Other factors may influence Class engineering, survey and audit, building on the new capabilities included within automated and cyber-enabled systems. Increased presence of sensors, with accompanying data capture or aggregation, and data analytics applied to the sensor data streams, should help to accelerate the engineering, survey and audit of cyber-enabled systems. Full utilization of sensor outputs can help to show system verification, fault tolerance, system resilience and data management methods. Additional analysis and system testing may be required to provide software assurance as part of software integrity analysis.

Other imaginative uses of sensors and data feeds beyond safety, reliability, security management and measurement may have transformative and advantageous effects at the asset level for Smart Ship owners and operators. Data capture and analysis should provide the added advantage of allowing condition-based assessments. If the components, systems, and assets are (1) engineered to provide data supporting monitoring, and (2) managed and maintained to ensure data continues to flow toward analytic mechanisms, then condition-based and risk-based assessments naturally follow as capabilities the owner or operator can leverage. This may enable timing and phasing of out-of-service periods, e.g., drydocking noted above, to be based on actual conditions and actual operating risks, rather than on simple schedules. Figure 5 below conceptually shows where schedules for docking may stretch periodicities based on actual conditions.

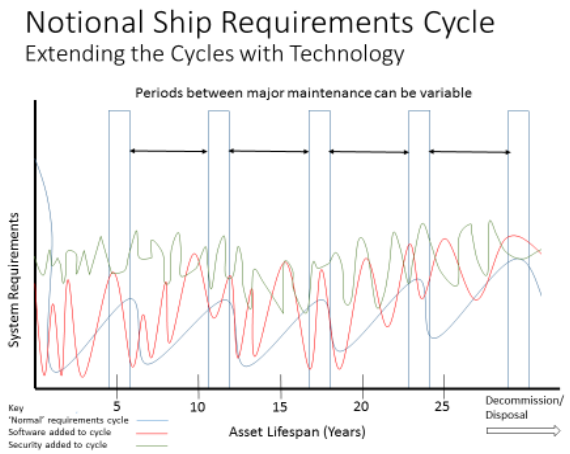

Figure 5: Conventional ship requirements and out-of-service periods (drydocking or overhaul) may be stretched with the data that can be harvested and analyzed from Smart Ships. System software and security requirements would continue to flow at the same rate, though major maintenance periods would be required on the basis of actual condition or measured risk, rather than on calendar marks.

4. CONCLUSION: THE WAY FORWARD

Class has a sound foundation to move into the Smart Ship era with owners, operators, crews, Flag States, and other industry participants. The key to Smart Ship examination and survey will be to concentrate on sound system engineering principles, executed in a phased approach to ensure that knowledge about the asset grows at each analysis, while keeping human and system safety foremost.

Class will use a consistent approach to identify and assess existing, available processes and tools in fulfilling its normal role (*safety, environment, public interest*) for Smart Ships, estimating *'what industry specific needs and abilities need to be provided by Class'.* However, Class need to be aware that marine industry requirements and the checking of those requirements will only be one part in a larger effort. For example, marine users will be only a small fraction of all users of most operating systems (even industrial ones) so the remedies that are developed for the main body of users will also need to be part of the solution for Class in Smart Ships.

The marine industry will continue to innovate to derive benefits (both obvious and as yet unimagined) from the interconnection of cyber-enabled systems. In the meantime, it is likely that the early adopters (or their regulators) will seek some formal assessment that accompanying risks have also been evaluated and considered acceptable. It is prudent for Class to seek rigor in these assessments in order that the evaluation can be reexamined in the future when unexpected risks are revealed or developed. This rigor will help provide reassurance at the time when the benefits are being realized but will also form the foundation for subsequent reexamination, incorporating both actual outcomes as well as lessons learned from other specific instances. Reexamination would be less objective if the process was not well structured, complete and documented.

Understanding the cost of proper assessments will, to some extent, offset the apparent 'top line' benefits from the capabilities of Smart Ships and will assist in budget decisions. But greater reliability and condition-based understanding of vessels will provide benefits to asset owners that will be quantifiable after taking life cycle considerations into account.

An understanding of the whole risk process (visualized better through the use of the bowtie approach) will also help determine the best balance of *prevention* and *post-event response measures*. The industry does not yet have sufficient experience or data to know where that balance should be struck. It may be that each vessel, or owner will arrive at a different point on that scale or it may be that all of industry gravitates to the same equilibrium point. This point may also be influenced by statutory requirements for back up manual control, irrespective of the precautions in place. It is envisaged that the

requirements for those manual back-ups will not be removed until the Smart Ship model is mature and there is sufficient data to demonstrate that they are no longer required.

Class' role in the Smart Ship concept, as with all new technical developments, is to apply its technical competence and industry-wide experience to determine the risks and hazards, and to provide a framework for practical and appropriate safety infrastructure without unduly restricting the potential for progress.

5. REFERENCES

[1] Notable exceptions to this are the new radio-communication technologies such as voyage data recorders (VDR), which can be retrofitted with the minimum of disruption to the 'as built' vessel.

[2] See International Safety Management (ISM) Code at http://www.mpa.gov.sg/sites/port_and_shipping/shipping/flag_administration/international_safety_management_code.page as an example.

[3] Requirements have many connotations through the engineering disciplines. In this context, the requirements cycle refers to the recognition, approval, accumulation, and satisfaction (installation) cycle that can be applied across generic systems.

[4] Moore's Law continues to show that the number of transistors that can be placed on a unit of space doubles every 24 months – implying that processor power or speed does as well. This observation has, in turn, driven rapid computer evolution and technology replacement for the past 40-50 years. Risk factors associated with rapid changes in technology can be accompanied by security weaknesses, personnel training or technology acceptance problems, or process development issues. Organizational Change Management (OCM) processes must be integrated with any major technology initiative to ensure the organization and its personnel can accept, understand and operate new systems without causing new problems.

6. ACKNOWLEDGMENTS

Thanks to Messrs. Rick Scott and Graham Marshall of ABS for their reviews and inputs to this paper.

7. AUTHORS BIOGRAPHY

George Reilly has been with ABS for 27 years and is currently a Managing Principal Engineer in ABS' London Engineering Department. He is responsible for reviewing developing technologies and their integration into the ABS Class process. His previous experience includes Shipyard Electrical Design Department, Class Electrical Surveys, technical review in London and Houston, contributor to the first ABS Guide for Dynamic Positioning published 1994 and while in ABS Houston - Marine Technology Electrical Department, the update of the 2014 Steel Vessel Rules Electrical and Automation requirements.

John Jorgensen is Director for IT Security at ABS. With formal education in communications engineering and IT management, extensive training in systems engineering, and three decades of security experience, he has worked in a variety of positions in the U.S. Navy, at the MITRE Corporation, and at ABS. He currently works at the ABS headquarters in Houston, TX, USA, with oversight on system and information security affairs across the ABS enterprise.