Working Document of the NPC Study
Dynamic Delivery –
America's Evolving Oil and Natural Gas Transportation Infrastructure
Made Available December 12, 2019

Topic Paper #4-16

CYBERSECURITY CONSIDERATIONS RELATING TO RAIL TRANSPORTATION

Prepared for the

Technology Advancement and Deployment Task Group

On December 12, 2019 the National Petroleum Council (NPC) in approving its report, *Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation Infrastructure*, also approved the making available of certain materials used in the study process, including detailed, specific subject matter papers prepared or used by the study's Permitting, Siting, and Community Engagement for Infrastructure Development Task Group. These Topic Papers were working documents that were part of the analyses that led to development of the summary results presented in the report's Executive Summary and Chapters.

These Topic Papers represent the views and conclusions of the authors. The National Petroleum Council has not endorsed or approved the statements and conclusions contained in these documents, but approved the publication of these materials as part of the study process.

The NPC believes that these papers will be of interest to the readers of the report and will help them better understand the results. These materials are being made available in the interest of transparency.

The attached paper is one of 26 such working documents used in the study analyses. Appendix C of the final NPC report provides a complete list of the 26 Topic Papers. The full papers can be viewed and downloaded from the report section of the NPC website (www.npc.org).

This page is intentionally left blank.

Topic Paper

(Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure)

4-16	**Cybersecurity Considerations Relating to Marine Transportation**
Author(s)	**John Jorgensen (ABS)**
Reviewers	**Al Lindseth (Plains All American Pipeline)** **Marty Willhoite (Miller Consulting Services)** **Wesley Malaby (Phillips 66 Company)** **Doug Sauer (Phillips 66 Company)** **Jay Churchill (Phillips 66 Company)**
Date: October 18, 2019	**Revision:** Final

SUMMARY

Marine cybersecurity requirements revolve around two main factors: system reliability for safe operations, and holistic security that encompasses the broad view of protecting the crew, ship and cargo. Mariners and operators need ways to understand the integration of cybersecurity in their greater context of transportation and cargo handling functions. This paper addresses an approach that merges cybersecurity with ship operations.

1. Marine Systems, Cybersecurity and Safety

Maritime community members – owners and operators of ships, offshore platforms and assets, regulated and process control facilities, and seagoing systems – have embraced automation systems as important elements of their assets and activities for the past two decades. Automation systems take the place of human activities, sometimes increasing the amount of work to be done in a task, and at other times replacing the human effort entirely. Transportation, cargo management, resource extraction, product processing and refinement, and vessel operations activities all

depend, to some increasing extent, on automated systems. Automation systems have been regulated by marine Classification Rules within the last decade[1].

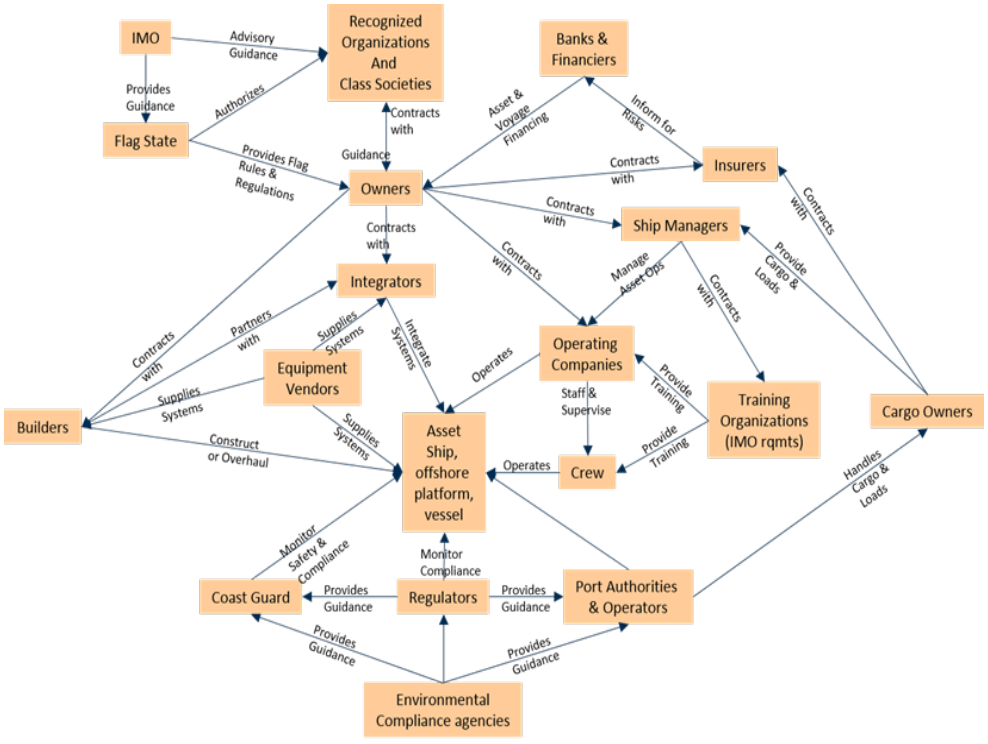
Computerization of automation systems has increased the efficiencies and effectiveness of processes in shipboard and processing facility environments. Automated systems onboard a typical large cargo carrier (ship) may include the following, in varying degrees of criticality to the ship and crew:

- Gyrocompass or inertial navigation system
- Autopilot
- Voyage data recorder
- Radars and contact management system
- Electronic chart display and information system (ECDIS)
- Global Positioning System (GPS)
- Automatic Identification System (AIS)
- Intrusion detection system (IDS)
- Power management system
- Vessel management system
- Digital twin and data historian
- Environmental controls (HVAC)
- Machinery control systems (MCS)
- Watertight doors
- Steering gear
- Propulsion control systems
- Cargo elevators
- Cargo cranes
- Bow thruster
- Mooring winches / deck gear
- Electrical generation and distribution
- Fire detection system
- Motor operated valves

[1] See ABS Rules for Building and Classing Marine Vessels, Part 4, Chapter 9 (Automation); see also International Association of Classification Societies (IACS) Requirements 2006/Rev2, Unified Requirement 22, "On Board Use and Application of Computer based Systems," 2016.

The operational and technical mission functions in a shipboard environment are the recipients of risks introduced by automated systems. Because of the large number of participants in the marine ecosystem, including owners, operators, crews, cargo owners, transhippers, Flag States, regulators, and more, automation tends to affect many members of the community, crossing functional boundaries to provide value chains in many new areas.

Figure 1 provides a representation of the marine community and some of the applicable interfaces. It shows connections and the notional relationship flows across the marine community. Automated flows, both of functions and of data (or documents), integrate some of the relationships, deepen or broaden others, and add largely invisible communications paths that support the operations of the community, and of marine transportation as a domain.



Source: American Bureau of Shipping, 2017

Figure 1: Marine Stakeholders and Notional Interactions

Various participants in the marine community will possess some or all of the typically automated systems. Ship and offshore platform owners and operators find these systems onboard their vessels; process control facilities and terminals will have control systems and information systems; vendors and integrators will enable data and control flows; and every responsible party will have needs for visibility and status or condition reporting for their systems, for their business functions, and for their exchanges with others.

These automated systems on vessels, which are more and more cyber-enabled with communications paths and standardized communications protocols, can increase work capacity in a company or crew, while also increasing relative safety of personnel, ship, systems and environment. But there are factors required to ensure safety over time, and these become precursors to the security needs for safety to be reliable. System knowledge is critical to safe and efficient operations. Networked and communicating ship assets (systems or components) must be known, catalogued and tracked, documented and managed. Because ships are one-of-a-kind products, and they are most often used away from their building yards, there is seldom an opportunity for corporate knowledge to be developed and managed at central shipyard or maintenance locations. Ship systems are installed or removed for function, investment returns, or efficiency, generally not according to a master lifecycle plan. Often documentation lags installation, and configuration requirements may be only maintained by pass-down knowledge in crews.

Communications paths must be known and controlled to ensure networked or connected assets are protected as they work with other components. Understanding how and why components may communicate is vital to managing those assets[2]. Personnel and machine access points (and authorized identities associated with access means and methods) are key to managing communications with connected assets.

[2] An example of communications controls may include remote cellular communications implemented on a ship engine, activated by the engine operating program to report performance data back to the original equipment manufacturer (OEM) when the system detects mobile signal (i.e., is close enough to land to make connection). Remote access communications must be known by the owner / operator, documented and trained to ensure the crew knows how to handle the communications links safely and securely.

2. Building Cybersecurity into the Company

With knowledge of automation systems, communication paths and the identities authorized to access the systems and communications, the organization can conduct a risk assessment of its operations and assets, governing results and decisions for prioritization of efforts put into cybersecurity, software-based systems, and operational capabilities that include computerized automation systems.

Real security begins with understanding what the company owns, how it communicates, who can touch it, and how risks are handled in conscious decisions. The company can then set goals for security. Not cybersecurity, specifically, but overall security for the company, its ships, facilities, and people.

The goal-based approach to security is conceptually similar to the International Maritime Organization (IMO) goal-based approach to safety. Goals bring objectives, which can be measured, and then objectives spawn projects and tasks. The measures that indicate progress also show where goals are achieved, or where gaps remain. The same approach can be used for security. Perfection is not the outcome of the security program, but sustainability can be, if the goals are met.

When automated systems are connected into systems of systems, and then into complex systems of systems, the goals associated with security can become diffuse. That is when the principal requirements of system knowledge, communications management, identity and access management, and risk assessment must be used to guide the program. These are not technical issues, per se, but many organizations treat them as such.

The concepts are often muddled among asset or access management, and technical configuration or verification of settings. Many shipping and offshore companies contract with third-party vendors for the management and care of their cyber-enabled systems, often leaving their own personnel without the comprehensive knowledge or specialized training needed to monitor performance, anticipate faults, preempt failures, and recover from downtime. The more organizations that are involved in system operations and maintenance, the more diffuse the responsibilities for care and management of those systems become.

When it comes to running the business, documentation of ship systems, with system diagrams, response plans, casualty control procedures, and safe-operation parameter permissives, becomes a lower priority than moving cargo, operating the ship, or making compliance reports. When technical systems are broadly managed by many organizations, security goals are often submerged with the documentation backlog, leading to losses in corporate knowledge. Security goals depend on understanding assets, how the assets communicate, who can touch the assets, and how risks are handled.

Access management and control becomes a difficult issue if a company does not spend adequate time defining job requirements, data or systems access needs to satisfy job needs, and the machine (i.e., automated entities) accesses that will transfer data without human intervention. Identity management relates closely to access control, and this requires Information Technology (IT) administrator, and Human Resources or Personnel Department interaction across the operational technology departments to address enterprise-wide solutions.

Identity management can include personnel background checks, badging, access allowances or grants, user identification and naming conventions, system logon credentials and controls, multi-factor authentication registration and management, and system logon or access recordkeeping and reporting. Ideal identity management makes coherent recordkeeping across the organization a characteristic of systems and global administration, simplifying system logons for users while providing consistency in logs, records and management.

Identity management must also extend to machines that are authorized to access other machines' data and operations. Each entity that communicates in a network must have consistent naming and behaviors identified, codified and enforced through policies, tracked and managed through logs and records, and audited for execution. Software accessing other software will sometimes exhibit unpredicted behaviors, so it is important that system administrators and system managers use consistent naming conventions – across all users, human and machine – in support of system management. This is especially important when outside entities, including vendor organizations or data harvesting utilities, have access grants to company data or systems.

Physical access is a vital aspect of access management. This includes ship, plant, facility, offshore asset, wharf, port terminal, transporter, and vessel accesses, as one would expect. It also

includes physical contact control with systems equipment, data stores, system and process controllers, system software, communications ports, sensors and communications messaging with both systems and people. Transportation Working Identification Credential (TWIC) is a US Government requirement for physical access to facilities and vessels; owner or operator credentials must be issued and used for personnel inside the facility or vessel perimeter. Company policy is necessary for the organization to balance internal requirements with external physical security. An access policy and associated access methods are then completed by use of authorization policies and access controls that leverage the company's technology systems for traceability, accountability and tracking across systems, and across time and geography.

Vendors and system integrators or providers gain or exercise physical and logical access in maintenance and shipyard periods: installation, checkout, troubleshooting, and initial operations are all within the scope of most third-party provider contracts. Further maintenance and support contracts, especially for software-intensive systems that require annual support for updates, are the rule, rather than the exception, for automated systems and for complex systems of systems.

Third-party vendors and providers are trained and contracted to keep automated systems groomed and operating for owners. They will also maintain configurations and check for equipment performance and safety issues. Increasingly, they perform these duties remotely when the systems they provide are connected to communications lines to the Internet. Because the non-crew vendors and providers have intimate access to systems, sometimes without complete supervision if crew is performing ship-wide evolutions such as onloads or offloads, it becomes more critical that the company contracting with the non-crew organizations perform due diligence in screening the vendors and providers. Remote vendor access to systems is a much more common occurrence with the prevalence of Internet of Things (IoT) and cellular connections on systems. Because valuable functions are sometimes made available with remote data streams and remote command access, owners allow more remote connections – which is another reason why vendor screening, and the trust it can bring to contractual relationships, is more important than before.

Increasing commonality of networking, and growing component density of connected systems, while communicating with industry-standard protocols, on commercial transmission paths, accessed by a mix of company and external personnel, using logical accesses that may be

remote – the vessel network becomes a complicated place to operate. The growing reality of shipboard connections or networking increases owners' and crews' abilities, but with a renewed need to understand how those systems connect and operate when connected.

Risk assessment becomes the next security program activity, once assets, communications, and accesses and identities are understood. The risk assessment process is conceptually simple – what might happen, under what circumstances, and what can be done to prevent it. When automated systems are included in the vessel's operational capabilities, the process of understanding risk requires more rigor than with conventional approaches.

When marine vessels and platforms network their sophisticated systems, and they may connect these systems to other networks. Risk assessment accounts for both connected and standalone systems, considering their potential or expected failure modes, and how those systems can affect people, systems, the vessel or the environment. When automated systems are included in the risk assessment, new variables associated with control can affect outcomes. Hardware reliability, software operations modes and fault modes, security postures, error conditions, and data interactions or dependencies with other systems must all be considered as part of the risk assessment.

When the automated systems have effects on vessel operations, with safety implications, they must be tracked differently than purely electro-mechanical systems. Events or incidents resulting from automated systems failures can introduce larger implications for operational safety than relatively simply material failures. Root cause analysis processes must now include, at a minimum:

- Material failure effects
- Unauthorized access (human or machine/software)
- Software errors or interoperability failures
- Human error
- Automated system failure (multiple causes)
- Data dependencies and data integrity issues

These factors are in addition to the typical root cause analysis causation factors[3], and a rigorous view of automated system causative factors will address many more than this brief list.

With causative factors in mind, an owner can then implement tracking and management of automated systems in order first, to manage automation systems (hardware, software, cyber-physical systems, firmware, mobile systems, etc.) in ways that allow integration of common skills and technologies, and second, to link cyber-enabled systems that can affect safety to the Safety Management System (SMS) required by the International Maritime Organization (IMO). The first priority is a Cybersecurity Management System (CMS) that can aggregate all automation-related systems into a comprehensive management system for use by owner, crew and maintenance personnel. Such a management system will allow the owner or operator to capture assets, communications and access allowances and permissions into an aggregated document or set of artifacts that will contribute to crew knowledge and capabilities. The concept of CMS is slowly gaining a position in the marine community as of this writing. The connection of cyber-enabled systems, cybersecurity and safety has been mandated for integration with vessel Safety Management Systems by 2021[4].

Technical domains, including Information Technology (IT) and Operational Technology (OT), are converging as this steady technology transformation occurs across the maritime community. The connection of one technology type to another, with associated communications protocols and paths, brings further complexity to an already complicated environment; technical personnel with experience and depth in IT are seldom trained in the operational, industrial control and process control technologies due to the separations in utility and uses. Likewise, the physical isolation and specialized nature of OT components and systems, and the particular training required for these systems by OT maintenance personnel, tends to separate them from the conventional IT and information systems that are nearly ubiquitous. Integration of IT with OT, to allow software updates on process control systems, pull performance data from operational

[3] See the ABS Publication *Guidance Notes on the Investigation of Marine Incidents – 2005* (publication 142, updated February 2014, available at ww2.eagle.org) for a comprehensive approach to incident causation.

[4] The Maritime Safety Committee of the International Maritime Organization adopted Resolution MSC.428(98) in June 2017, encouraging administrations to ensure that cyber risks are appropriately addressed in existing SMS no later than 1 Jan 2021.

systems, or provide monitoring and visibility of the OT systems, also allows accesses to OT in new and novel ways. Remote accessibility, previously mentioned, addresses companies' monitoring and management priorities, but at the potential cost of opening remote industrial control systems to unexpected human or machine contact. Heterogeneous technology integration requires more specialized training and background for effective development of architectures, suitable protective systems, and efficient operational capabilities.

As systems and technologies converge, business and operational mission processes and procedures change to fit the technologies and accompanying capabilities. The company knows its systems, their communication requirements, its personnel and machine accesses and identities, and their relative risk positions. The company governs changes in the processes supporting systems and company assets, thereby to provide decisions on how the company employs its automation systems best. This step is implementing management of change, which is a critical aspect of governance and asset management processes, but which is often neglected. Management of change is that process by which a company governs its technology across the entire breadth of the organization, aligning technology and tools with the work processes and end outcomes that bring business and missions to successful conclusions. Cyber-enabled systems are software-intensive, and investment decisions concerning replacement or update of automation systems are distinctly different in comparison to replacement or update of mechanical or electro-mechanical systems. Automation system updates are frequently performed because of new functions available in the software, though many updates are driven by security patches or obsolescence; conventional equipment replacement or update is often only performed for economic reasons. The strong difference becomes grounds for new processes in the organization, if the company accepts the need to treat software-intensive systems differently than non-software-containing systems.

An important aspect of management of change directly relates to software. The ease by which software can be replaced in IT systems tends to bias managers to expect the same in mission-critical (bridge or propulsion) systems, and sometimes in process control or industrial control systems as well. Software management of change is more than deciding to update from version 3.2c to version 4.0.1 in the enterprise resource planning system: it also includes the human policy decisions about allowing vendors to make software updates to systems without documentation;

decisions to require testing in largely similar environments prior to installation; and documenting the functions, failure modes and casualty control requirements associated with the new software.

Management of change also extends to the policy basis for security in system operations. It can include the decisions behind security controls, such as whether USB portable storage and drives will be allowed for use [5], and under what circumstances they might be used in a system. Security controls are subject to management of change in all respects, considering the organization's assets, its communications needs, the way it allows or regulates access, and its risk posture and outstanding risk conditions. Management of change, for all automation systems, addresses the decision processes behind security governance.

Governance and management of change both include training and procedural updates for organizational personnel and processes. The automated systems used on a vessel, or in a process control facility, should be documented and regulated for physical, logical and remote access methods. The personnel with access to those systems are a singular source of error to automation, whether by simple mistakes in operation, or by misunderstanding of procedures, or by incomplete training. Most errors – 90 percent of all system malfunctions – found by or reported to the American Bureau of Shipping (ABS) cybersecurity assessment teams are attributable to human error[6]. System updates and automation installations require documentation, training, system validation and verification, and failure mode documentation for inevitable events and incidents.

An important part of failure and casualty control procedures is the backup, or failover, procedures. Business-critical or mission-critical systems require advance planning for business continuity and vessel/personnel safety in the form of backup procedures. Manual backup procedures complement smart system acquisition procedures. An example illustrates this principle most clearly. An oceangoing ship's bridge is required to have dual Electronic Charting Display

[5] With implications for security, of course; the example of the Chinese citizen apprehended on 2 April 2019 with a thumb drive containing malware, on the President's estate in Florida, illustrates the ever-present danger of unexpected intrusive software that may place trusted systems at risk.

[6] Operational knowledge from ABS teams, 2018.

Information Systems (ECDIS) and Global Navigation Satellite System (GNSS) receivers, for example. If the owner procures identical units for ECDIS and GNSS, she/he may save on procurement (numbers discounts) and training (similar units streamlines training); but that becomes false economy if both ECDIS units are susceptible to the same software vulnerability, or both GNSS receivers are spoofed in the same way to deceive the bridge crew. Effective backup procedures would call for dissimilar systems for the same function, with personnel trained in manual piloting and open-ocean navigation techniques. In this case, thinking through the resilient solution, i.e., considering potential failures and thinking through countermeasures, helps to minimize risk while providing ship and crew with a higher likelihood of favorable outcomes. Secondary, often manual, methods for accomplishing critical functions are important additions to risk assessment considerations.

The final area to consider is that of interfaces between the ship and port terminals for data exchanges involving cargo management operations, including inventory, onload and offload. The data-dependent systems on vessel OT must be able to communicate with data handling systems at production or terminal facilities. Because convergence of IT and OT is often the solution to data interoperability, communications becomes a standards issue of potential concern for interoperability and security. Ports and terminals may have a significant role to play in determining the protocols and content of standard messaging, if the data management between ships and terminals can be seen as both enabler for commerce, and as a critical parameter for operating safety.

FINDINGS

1. **A goal-based approach to security is understandable and useful, once the concept is elucidated to end users.** Once owners and operators understand the automation systems upon which their business processes depend, they can begin security development. Security implementation with any framework (e.g., NIST CSF) is more complete and understandable within the context of a goal-based approach, supporting their business processes and crew functions, rather than as a compliance-based approach. Not every organization can implement every control; a goal-based approach encourages strategy and goals to inform actions at each step and each stage of maturity.

2. **Asset identification and management are critical aspects of any cyber program.** Those systems, components or functions that connect to networks or networked systems must be known and understood, whether as functional parts of processes, or as infrastructure. System complexity, especially when documentation is incomplete or inaccurate, makes control and management of cyber-enabled and cyber-physical systems very much more difficult. Asset control does not just have financial implications; it has control implementations for systems that can cause physical effects to systems, to people, and to the environment.

3. **Connections and communications must be known, documented and maintained as critical parts of system knowledge with any organization that owns automation systems.** External communications links and transmission lines affect asset management and control, and they must be positively controlled as organizational assets.

4. **Documentation and corporate knowledge for systems and automation functions in any organization are critical to the understanding, management and control of automation systems, cyber-physical functions, and safety-critical systems.** Too often, however, automation systems do not have continuity and completeness in the owning organization's documentation and log keeping activities, which leads to unknown hazard or safety conditions that must be continually relearned and reassessed.

5. **Access control for physical access (facilities, ships, terminals, vehicles, etc.) is fully as important as logical access for all automated systems.** Access control depends on personnel investigations and security (through Human Resources); physical security; physical surveillance; and identity management and authorization (which requires partnership among technology, operations and HR departments).

6. **Owners, operators and crews often show less in-house knowledge of control systems in their production systems when the controls are cared for exclusively by third party subcontractors.** Owners and operators must emphasize system knowledge and control system understanding in order to ensure organizational capability to control and respond to system events, while making optimum use of third-party contracts and partnership arrangements.

7. **Identity management is a critical, but under-emphasized, aspect of access management that requires more granular attention. Identities of human and machine entities that**

are allowed access to assets, controllers, data or operations, must be known, controlled, resolved and tracked through operational cycles and system contacts. In this way, organizations with automated systems may assign attribution to control access events, track those events through protective systems, and correlate events to likely contra-indicators for authorized accesses (e.g., geo- or temporal filtering for identification of stolen credentials).

8. **Logical access control, including both local and remote system or data access, starts with physical access control and identity management, and then expands to job requirements and definitions of access needs to support organizational requirements.** Authorizations for access must be conscious decisions that are supported by identity management, and then decided by personnel job requirements, physical accesses, subcontractor security vetting, and personnel training and certifications.

9. **Vendor screening, whether for procurement agent vetting, for data processor authorization, or for verifications of third-party maintenance and contracted system care companies, is important to organizational confidence in contracted or partnered companies.** Third parties who come into contact with organizational assets, whether functional (cyber-physical) or logical (data stores or data streams) must have the system owner's interests in mind prior to being allowed access; but the owner must take steps to train or indoctrinate third parties for safety and security expectations prior to access being granted.

10. **Risk assessment activities are periodic and continuing requirements for all production, transport and storage organizations.** Automation systems increase both efficiency and potential risks in any organization, and risk assessment / risk management efforts must include the potential effects of automation systems on safety, security and operations of the owning organization, its people, and the environment.

11. **Risk assessment helps with recognition of events / incidents by encouraging knowledge of failure modes and potential systemic effects of malfunctions, failures or malevolent actions**. Events and incidents, when recognized as potential results of system disruptions, can be included as integral parts of monitoring technologies and routines, and they can be anticipated in organizational casualty control procedures.

12. **Automated systems that may affect safety, whether human, system, ship or facility, or environmental, must be included with management of both cyber-enabled systems, and with safety management.** Safety of automated system operations and effects, in any production or operational environment, depends on security of systems and data flows, on integrity and availability of data, and on positive control of the systems at all times.

13. **Integration of IT and OT requires specialized knowledge of system characteristics and operation, and new understandings of protective mechanisms, in order for companies with converged architectures to keep their functional systems safe and secure.** Integrating from information technology (IT) to operational technology (OT) may provide efficiency and effective operations, but the communications and protocol complexities thereby introduced add considerably to the load on human operators and maintainers to understand, interpret and manage. Special skills are required by integrators to add effective

protections to hybridized architectures, both on ships or offshore assets, and to facilities that communicate with those assets.

14. **Continued automation of processes - because the technology allows it - is not matched by changes in education and training for crews or staff.** Integration and subcontractor work efforts often introduce new systems and processes that can revolutionize owner or production system operations; but the too-frequent lack of documentation, with incomplete training and coverage for understanding and management of the new systems, can make safety and security management much more challenging. Any automation system must be preceded by training and integration of new processes to ensure crew and owner knowledge support safety across all systems and operations.

15. **Management of change is a major organizational responsibility, especially for software-intensive systems.** Software or system management of change policies and guidelines support crew and system safety, and they ensure predictability and reliability of operations within the expectations of owner, operator and crew.

16. **Backup capabilities for automated capabilities, especially those with safety or security implications for ship or facility, crew or the environment, must be introduced, and crews trained, in each automation system integration project.** Backup capabilities must allow for regaining of system control and wind-down of operations to safe conditions, emphasizing those aspects that keep ship or offshore asset, crew and environment safe.

17. **Production and transshipping facilities must have compatible data and control flows to interface with ships / shipping / transport assets.** Interfaces for both IT and OT must allow data exchange; security protocol engagement; safety protocol enforcement; and status monitoring for the automation systems to serve crews and operators effectively.

18. **Federated systems (e.g., ports and terminals interfacing with transportation assets) must publish their interface requirements for data exchanges if they are to provide effective and efficient reception and forwarding of information content from shippers.** As automation systems and software-intensive systems, including sensor networks, are added to transport networks across ports, terminals and regions, the standards for communications, security and safety become principal contributors to operational safety across all stakeholders in the system-of-systems thus formed.

Recommendations: for Industry

- Encourage OEMs to provide digital and cyber characterization of systems to buyers, with service offerings for maintenance, software updates and vulnerability awareness alerts. Provide examples of reference architectures that show how integration of IT and OT may be performed with security in mind, depending on the documentation and knowledge of systems.

- Develop a model inventory structure for architectural asset compilation in a format that can become an industry standard, satisfy regulatory and insurance requirements, and provide understanding to organization personnel for those components and assets that require attention and care, even outside normal maintenance contracts and third-party arrangements.

- Form industry cooperatives among integrators and system builders to establish standards for documentation, system testing and turnover, and automation system behavioral requirements, the better to ensure familiarity with systems, knowledge of systems among owners and integrators, and common knowledge development across industry members.

- Develop model standardized contract language for communications and support requirements associated with automation equipment. Standard additions to contracts, meant to provide uniformity among expectations, may allow both gradations and phasing of cyber-enabled system additions or integration efforts on or in new ships, offshore assets, systems, facilities or terminals.

- Encourage software reliability and testability for safety and security by establishing behavioral standards associated with major functional systems.

- Develop and provide testing and assessment guidelines for automation systems, especially for cyber-enabled automation that is safety-critical or ship/function-critical, whether for the ship or facility itself, or for the environment.

- Develop an industry consortium to address staffing and training requirements, with guidance for common skills, transportable knowledge and industry-wide growth in capabilities associated with automation systems, safety and security.

- Continue working with US Government and US Coast Guard for improvements to the maritime industry-standard Transportation Worker Identification Card (TWIC) as a potential vehicle for wider authentication and authorization solution on ports, terminals, facilities and maritime assets of all types.

Recommendations: for companies and organizations

- Supplement asset management and control by segregation of networked assets where sensible and feasible, to ensure faults or failures in single systems cannot cascade or cause failures or intrusions across entire domains of process control systems or critical functions.

- Use hardware and software asset management to build software management of change requirements for all software-intensive systems, and especially for those with safety or security functions. Develop policies and training associated with management of change and of software to promote good practice and to remove potentially untested or incompatible software changes from operations and processes.

- Develop and use security and safety policies across all process control, machinery control or industrial control systems, using system documentation and asset and communications management needs to maintain corporate knowledge, current operations monitoring, and personnel training.

- Document and train, as part of Safety Management System (SMS) operation, the cyber-physical and cyber-enabled systems that can cause physical effects that may affect human, system, ship, or environmental safety.

- Document and train cyber-enabled systems as part of a Cybersecurity Management System (CMS) to track cyber-enabled assets or components, software systems and applications, and training requirements for maintaining security and safety of the cyber-enabled automation systems.

- Perform risk assessments of cyber-enabled and automation systems on a regular and scheduled basis, with direct input to the enterprise risk management program. Include potential failures of cyber-enabled systems (due to all causes) as inputs to enterprise risk impacts for risk planning and mitigation activities.

- Perform change management in all technical and staff process areas to improve sustainability of organizational capabilities, systems, training and staffing. No system, whether mission/business/function critical or not, should be modified without explicit consent from relevant decision makers in the organization - especially when such systems may have safety-critical effects on the crew, the ship or the environment.

- Conduct regular threat and vulnerability assessment activities as part of risk assessment and change management processes, ensuring the protective functions or architectures continue to meet (or exceed) the expected risks that may be posed against automation systems and the crews using them.

- Integrate configuration and patch management as part of risk assessment, change management, threat and vulnerability assessment and system maintenance work efforts. Document changes to configurations in system documentation, and ensure training reflects any major changes required in supporting new applications, operating systems, functional systems, etc.

- Regularly assess organizational requirements for functional backup capabilities and resilience needs, providing failover capabilities where required, sensible and feasible, and positive system control capabilities elsewhere. No function-critical process control system

can be allowed to fail if that failure results in safety or environmental issues, or in cascaded failures that can cause safety or environmental impacts.

- Prepared for adversity with incident response and recovery capabilities that include monitoring of critical components or parameters in all safety-critical automation systems.

- Perform physical security responsibilities in accordance with international law, national regulations, and prudent asset and crew protection guidelines. Physical security failures may not be allowed to bring cyber-enabled system failures.

- Use risk assessment, organizational needs and regulatory or statutory requirements to gauge the sufficiency and effectiveness of protective systems against threats endemic to the operating environment.