



Marine Board of the National Academies' Transportation Research Board

Cybersecurity and Safety: The Class Perspective

John M. Jorgensen

Director, IT Security
American Bureau of Shipping
JohnJorgensen@eagle.org
281-877-6675

**Spring Meeting at the National
Academies Beckman Center**

American Bureau of Shipping

More than a Century of Experience

- Since 1862, ABS has strived to meet the needs of the Marine and offshore industries. The ABS Rules incorporate the knowledge gathered from more than 150 years of operating experience and a continuing program of technological research.
- Statutory Recognition of ABS Standards
ABS serves as a Recognized Organization for more than 120 governments.
- These governments have recognized that ABS possesses a global network of exclusive, qualified surveyors and extensive resources in manpower and technology to act on their behalf to conduct the technical reviews, audits and surveys required by the flag State under applicable international conventions, national laws and regulations.



Classification Process

Ships, Marine Vessels, Seagoing Platforms

- The responsibility of the classification society is to verify that marine vessels and offshore structures comply with Rules that the society has established for design, construction and periodic survey.
- The ultimate goal of classification is to promote the safety of the passengers, the crew, the cargo, the vessel and the environment in which it operates.
- The classification process includes:
 - The development of standards, known as Rules
 - Technical plan review and design analysis
 - Surveys during construction
 - Source inspection of materials, equipment and machinery
 - Acceptance by the Classification Committee
 - Subsequent periodic surveys for maintenance of class
 - Survey of damage, repairs and modifications

ABS Philosophy on Cybersecurity

The mission of ABS is to serve the public interest as well as the needs of our members and clients by promoting the security of life and property and preserving the natural environment.

– ABS Mission Statement

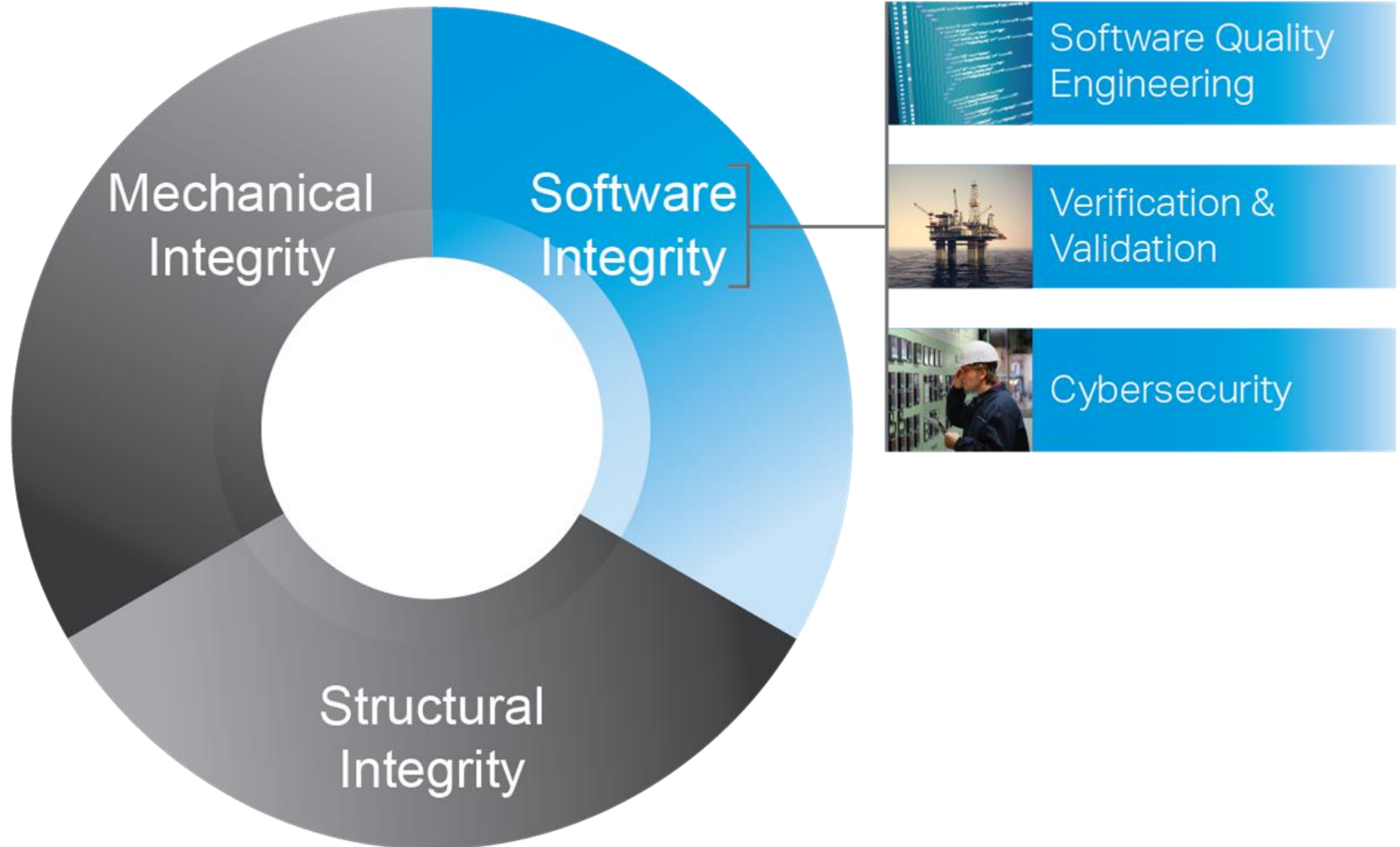
- ABS considers cybersecurity to be a critical factor in system, software and functional safety in marine vessels and offshore platforms.
- Cyber-enabled, software-intensive systems are ubiquitous throughout the maritime and engineering domains, and they affect all aspects of human safety. Cybersecurity must be factored into the architecture, design and engineering of these systems, which must be verified for both operating and failure modes to ensure human safety and security.

Some Available Standards

- International Society of Automation (ISA) / International Electrotechnical Commission (IEC)
 - ISA/IEC 62443 (formerly ISA99)
- National Institute of Standards (NIST)
 - 800-30, 800-37, 800-39: IT System Risk Framework
 - 800-53, 800-82, Cybersecurity Framework v.1.0
- International Instrument Users Association, Working Party on Instrument Behavior (WIB)
 - Process control Domain: security requirements for vendors, Version 2.0, October-2010
- North American Electrical Reliability Council (NERC) Critical Infrastructure Protection (CIP) v5
 - CIP-002 through CIP-009

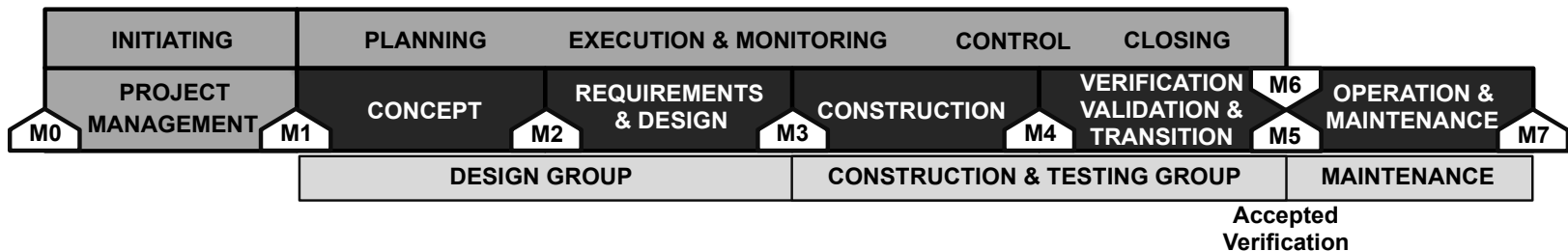


Software Integrity



Software – The First Step in System Assurance

- ABS and ABS Group Use Integrated Software Quality Management (ISQM) Methods to Assess Software and Processes
 - ISQM procedures and criteria rely on a structured process, based on best practices, for the engineering management of the software development process in the design, construction and maintenance of computer based systems.
 - Compliance with the ISQM process and criteria is intended to increase safety, accessibility, reliability, and ease of maintenance of computer based control systems.



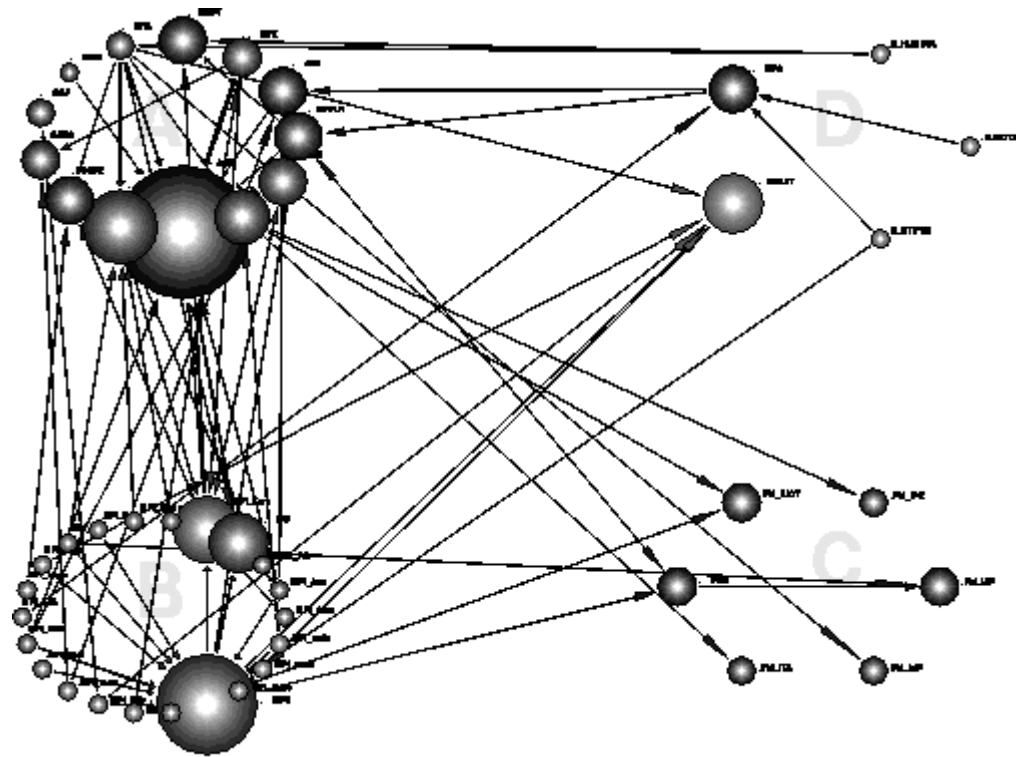
Source: ABS Guidance Notes, "INTEGRATED SOFTWARE QUALITY MANAGEMENT – CONFORMITY CERTIFICATION PROGRAM," Sep 2013

Control Systems Selected for ISQM on a Drillship



Approaching System of Systems Problems

- Boundaries at the System, Component, Module Levels
- Tiers of Failure Modes
 - Individual modules or components
 - Software dependencies
 - Input / output flows
 - Parallel flows
- Data Integrity is Vital
 - Unchanged since capture or authorized processing
 - In best case, indicates that systems can be trusted
 - In worst case, destroys confidence in systems



Source: <http://www.mpi-fg-koeln.mpg.de/~lk/algo5a/node13.html>

The Future of Offshore Automation

Unmanned Cargo Ships Face Industry Resistance, Are a Good Idea Anyway

By Evan Ackerman


Posted 27 Feb 2014 | 16:27 GMT

[Share](#) | [Email](#)



Image: Rolls-Royce

Source: Petrobras



AUTONOMOUS UNDERWATER VEHICLES

In addition to systems equipped with

AUGMENTED REALITY

features, cable-free robots are being tested to undertake **continuous** operation monitoring.

They will be fitted with sensors and controlled from **viewing rooms located on land.**

Students race for top prize in RoboBoat Competition

Published 30 July 2014

[+ Share](#) | [Email](#) [Facebook](#) [Twitter](#) [LinkedIn](#)

Obstacle avoidance. Automated docking. Speed gates. Acoustic beacon positioning. Underwater light identification. These are just some of the missions teams had to successfully complete to win at the 7th annual International RoboBoat Competition, held 8-13 July at the Founders Inn and Spa in Virginia Beach,

Threats to Systems and Function

- Threats to Function and Safety

- Operator errors in procedure
- Software flaws
- System intrusions by unauthorized access
- System intrusions by cyberattack methods

- Attack Surface

- Systems
- Data and repositories
- Personnel
- Processes

(Some) Methods to Mitigate or Negate Threats

- Operator training
- System performance monitoring
- Failure mode detection
- Access monitoring and management
- Software configuration control, including control of system and software maintenance
- System communications control
- Blocking of unauthorized communications
- Testing: predeployment, post-deployment, patches, upgrades, vulnerability and penetration

Cybersecurity is Fundamental to Function

System Functional Assurance Determines System Safety

Understanding the Problem

- Technology Is Integrated Into More Applications Each Year
 - System sensors and reporting mechanisms support Condition-Based Maintenance
 - Systems of systems boundaries encompass more functions as available interfaces bring new connections
- “Internet of Things” Grows Daily
 - Sensors report data from...everywhere
 - Cyber-physical devices transmit commands into action, and up-front certification for safety must be mandated
- Vehicles Are the ‘Next Big Thing’
 - Safety systems and condition monitors will be vital
 - Requirements and standards for manual system operational capabilities must be used to ensure safety

Cybersecurity is Fundamental to Assurance

System Functional Assurance Determines System Safety

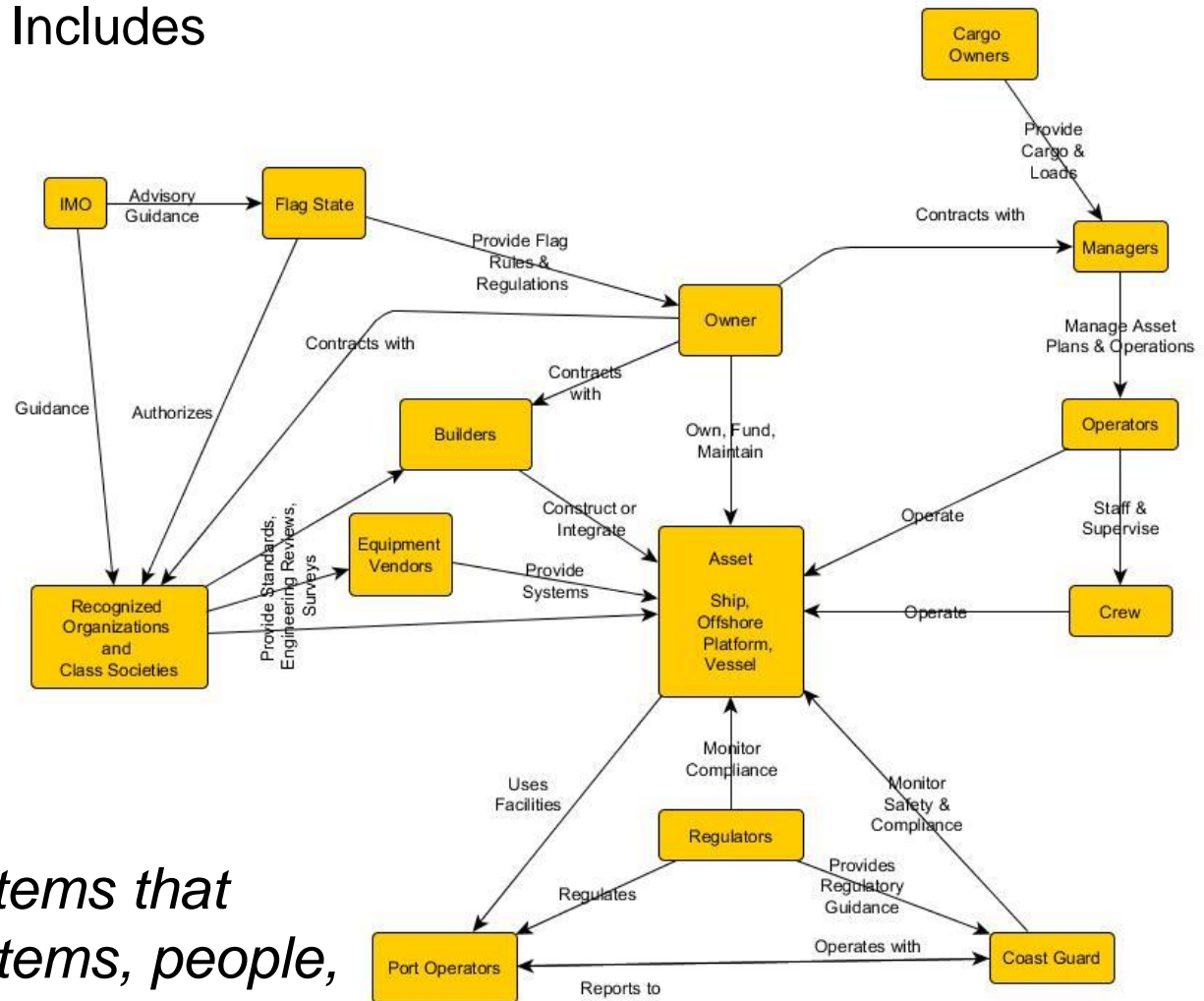
Solution Requirements Include

- Risk and Safety certification
 - Safety-critical system engineering language (Goal-Structuring Notation (GSN))
 - Failure Mode and Effects Analysis (FMEA) / Criticality Analysis / Program Protection
 - Deterministic risk analysis (e.g., Bowtie Analysis)
- Monitoring and management
 - Function tracking and condition management
 - Attribution determination and origination limitations
 - Intelligence and automated feeds for threat blocking
 - Data transfer tracking inside an organization
- Test & evaluation methodologies
 - Auditable software generation methodologies
 - Software testing tools & techniques
 - Failure modes discovery
 - Unified user interfaces in tools integration
 - Supply chain risk mgmt

Maritime Industry Interactions

- Basic Interaction View Includes

- Owners
- Builders
- Operators
- Managers
- Vendors
- Cargo owners
- Flag States
- Class Societies
- International Maritime Organization (IMO)



This is a system of systems that includes platforms, systems, people, processes, and data.

USCG Desired Outcomes – 1

- Maritime Safety Needs Drive Compliance Inspection Processes
 - Deterministic compliance testing with minimal exceptions
 - Ability to assess systems, ships, platforms and installations for safety, compliance and functional capabilities - including manual and backup capabilities
 - Understandable data flows on vessels and platforms
 - Maintain port flows, safety operations and enforcement capabilities
 - Maintain continuous C2 and situational awareness (including sensor feeds) for port and transit areas
 - Integrated training and personnel knowledge building with the instrumentation and operations packages
- USCG Standards Drive Collaborative Work With Industry and Community Partners
 - Standards (and inspections) for third-party and partner data management and security
 - Functional analysis of cyber protective requirements for ports and port authorities
 - Guide and templates for cyber response plans at ports

Desired Outcomes derive partially from 23 Apr 15 discussion with CAPT Penoyer, USCG, COTP Houston

USCG Desired Outcomes – 2

- USCG Systems Demonstrate Measurable Cybersecurity
 - USCG and USG needs drive acquisition processes
 - USCG systems are designed, manufactured and tested to understood risk
 - Functional assurance standards are required for any acquired or procured software, with tools and techniques to determine capabilities
 - System manufacturers and integrators have T&E methods and tools available to reach known and knowable operational risk conditions
 - Port systems are known, understood and fault-tolerant
 - Standards are in place for safety-critical systems
 - System requirements and architectural function collections across capability portfolios
 - Interfaces for data and agreements / SLAs
 - Internal USCG Standards Maintain Functional Assurance
 - Control and monitoring of internal systems
 - Methodology for vulnerability assessments

Recommended Areas of Research – 1

- Threat Research
 - Attribution methods
 - Automated threat information sharing methods
- Decision Support
 - Packaged monitoring capability
 - Identify decisions needed, with automated IR capabilities
 - Compliance measurement against vulnerabilities
 - Collaboration methods for complex operational condition management (knowledge sharing / effectiveness as a differentiator)
 - Out-of-box capability package for event flow (logs) capture and analysis, using open tools
- Automation and Human Factors Engineering as Reaction Accelerators
 - Automated system hygiene assessment
 - Event recognition and reaction automation
 - Human Factors Engineering (HFE) on dashboards, with a build framework and automated tools
- Encryption
 - "Cheap" encryption methods for Data In Motion (DIM) coverage
 - Certificate management across the enterprise

Recommended Areas of Research – 2

- System Acquisition

- Architectural development process to accompany SE
- System development milestones or checkpoints in SE that can accommodate cyber-enabled system convergence
- Application of set-based design to cybersecurity
- Technology refresh capability assessment: rules and guidelines
- Maturity and resilience generation as part of system development

Possible Standards

- Maritime controls and monitoring framework
- Verification guidance to provide measurable safety in systems and critical processes
- Testing and audit process guidance

- Testing

- T&E methods to increase knowledge of systems and their conditions
- Vehicle control systems safety test methods, and safety monitoring for measures
- Audit methodology for assessing third-party capabilities to protect any given information
- Data movement detection or surveillance counter-detection technical methods

- Assurance

- System interoperability standards
- “Bullet-proof” system assurance checks and standards
- "Friendly botnet" that absorbs known machines into the system with agents



www.eagle.org

December Q1: What cyber-dependent systems, commonly used in the maritime industry, could lead or contribute to a TSI if they failed, or were exploited by an adversary?

The screenshot shows the Federal Register website. The URL in the browser is <https://www.federalregister.gov/articles/2014/12/18/2014-29658/guidance-on-maritime-cybersecurity-standards>. The page features the Federal Register logo and the text "The Daily Journal of the United States Government". A blue banner at the top right says "Notice". The main heading is "Guidance on Maritime Cybersecurity Standards". Below it, it says "A Notice by the Coast Guard on 12/18/2014". There is a green button that says "SUBMIT A FORMAL COMMENT". Below that, it says "Comments on this document are being accepted at Regulations.gov". The "ACTION" section says "Notice With Request For Comments." The "SUMMARY" section says: "The Coast Guard is developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident. Coast Guard regulations require certain vessel and facility operators to conduct security assessments, and to develop security plans that address vulnerabilities identified by the security assessment. The Coast Guard is seeking public input from the maritime industry and other interested parties on how to identify and mitigate potential vulnerabilities to cyber-dependent systems. The Coast Guard will consider these public comments in developing relevant guidance, which may include standards, guidelines, and best practices to protect maritime critical infrastructure." On the right side, there is a "LEGAL DISCLAIMER" section and a "Font Controls" section with buttons for PDF, DEV, PRINT, and PUBLIC INSPECTION. The "Publication Date" is Thursday, December 18, 2014. The "Agencies" are Coast Guard and Department of Homeland Security.

Cyber-enabled systems can be vulnerable to disruption. Such systems which might cause

TSI may include:

- Integrated ship control
- Navigation and charting
- Machinery control
- Propulsion control
- Cargo handling
- Environmental control
- Third-party software and services

TSI: Transportation Security Incident

December Q5: What factors should determine when manual backups or other nontechnical approaches are sufficient to address cybersecurity vulnerabilities?

- Requirements for manual backup capabilities should be determined by the risk inherent in the failure of a particular cyber-enabled equipment. If a cyber-enabled equipment could cause hazard to either human or vessel safety through its failure, then that system should have either disconnected failover capability, or a manual backup system. Examples might include
 - Vessel steering (with After Steering manual takeover);
 - Main propulsion controls (through Central Control manual takeover); or
 - Generator operation (with manual operating ability).
- Further, backup capabilities must be out-of-band capable, not subject to the same vulnerabilities for which the primary cyber-enabled systems may have weaknesses.
- Some systems are so critical as to require special consideration – such as prohibiting automation – to prevent catastrophic risks
 - Reveal these through detailed risk analyses (e.g., Bowtie)

December Q7: How can vessel and facility operators reliably demonstrate to the Coast Guard that critical cyber-systems meet appropriate technical or procedural standards?

- Operators must demonstrate in cyber-enabled systems the ability to control:
 - Failure modes;
 - System status reporting; and
 - Data integrity for safety-critical systems.
- Operators must also demonstrate accurate situational awareness of cyber-enabled systems, to include auditable system status, log integrity, safety failover capabilities, and manual backup operations for critical control and safety systems.
- Recognized third-party accreditors may require demonstration to certify safety and correct operation of system