Risk-based appraisal of MASS performance – Considerations, challenges and possible approaches

MTEC ICMASS 2019

13 November 2019

Kie Hian CHUA, Technology Centre for Offshore and Marine Singapore

Dimitrios KONVESSIS, Singapore Institute of Technology

Imran IBRAHIM, DNVGL

Outline

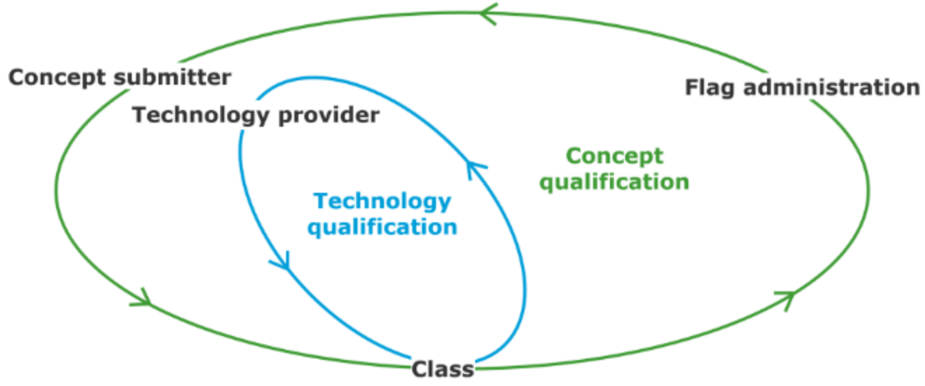
- Review of issues
- Aspects of safety verification that must be addressed
- Benefits & Gaps of Current Practice
- Potential methods to address gaps of current practice
- Future areas

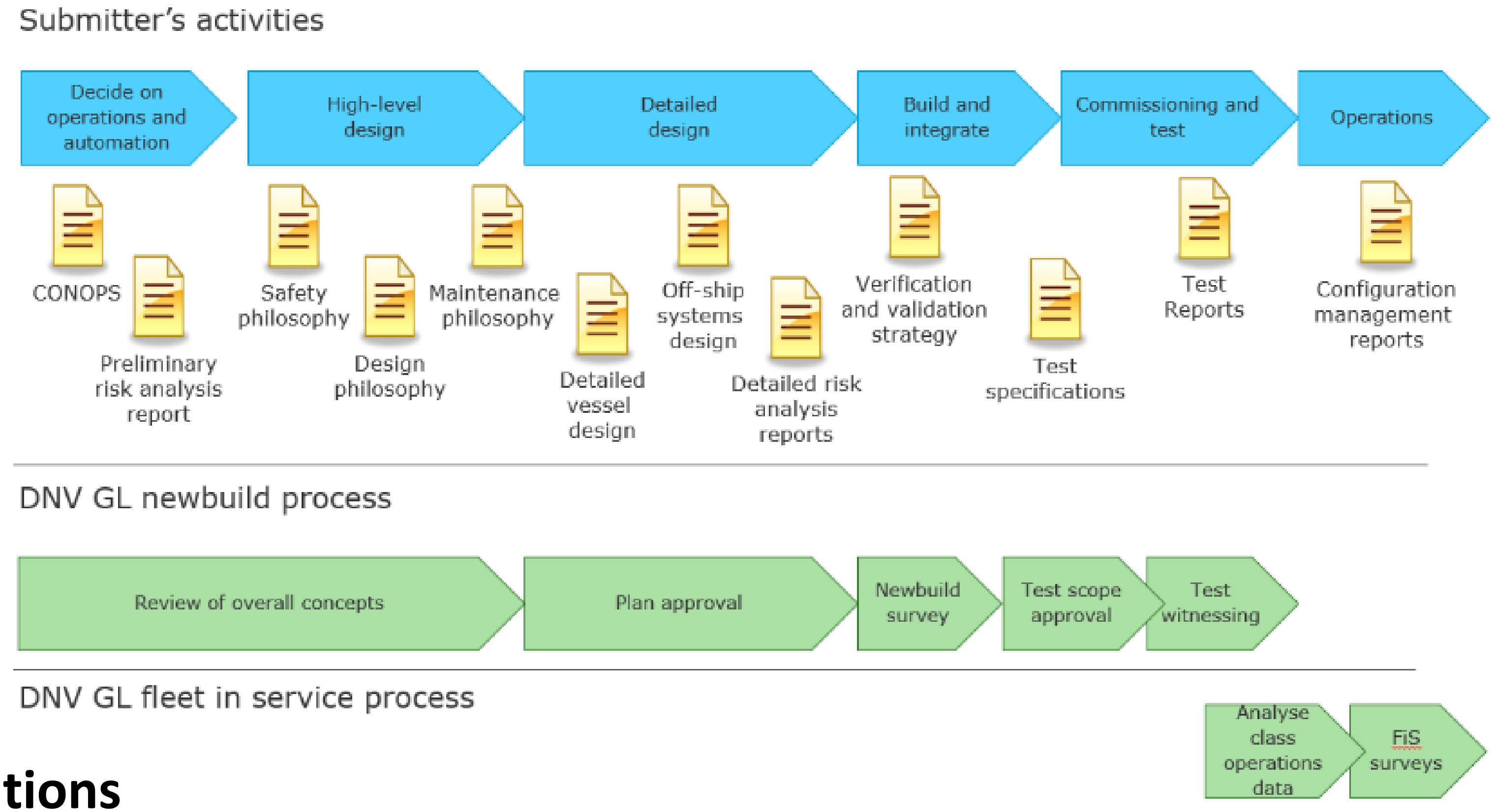
Review of Issues

- Novel concepts
- Equivalent safety
  - MSC.1/Circ. 1455
  - DNVGL CG-0264

  "When considering safety measures for a vessel, the risks … shall not focus only on consequences for the on-board crew, but also take into consideration consequences for the public, the assets and the environment."
- Risk-based approach
  - Need to go beyond reliability & component failures to overall risk to society
- Cyber-security & physical security need to be integrated

Concept qualification process: Example (DNV GL)





Submitter's activities

Decide on operations and automation → High-level design → Detailed design → Build and integrate → Commissioning and test → Operations

CONOPS

Preliminary risk analysis report

Safety philosophy

Design philosophy

Maintenance philosophy

Detailed vessel design

Off-ship systems design

Detailed risk analysis reports

Verification and validation strategy

Test specifications

Test Reports

Configuration management reports

DNV GL newbuild process

Review of overall concepts → Plan approval → Newbuild survey → Test scope approval → Test witnessing

DNV GL fleet in service process

Analyse class operations data → FiS surveys

DNVGL CG-0264:

Integration of Tech. and Concept Qualifications

- New op. concepts based on developing technologies
- Properties of technologies will be scrutinized on pilot vessels
- Operational concepts adjusted accordingly

Aspects of safety assurance to be addressed

- Different models for autonomous transformation
  - Phased transformation: Conversion of existing tonnage
  - “Multi-level” vessels
- Remapping of roles (responsibilities) & evolving human-machine interfaces
  - Beyond crew to different stakeholders
  - Need to consider socio-technical dimension
- “Equivalent safety” is not a constant
  - Systems with self-verification?
  - Learning systems
- Verification of intelligent systems based on AI / application of ML
- Proprietary “black boxes”
- Reliability vs Safety

Examples of challenges to be addressed

Decreasing accident levels: what is equivalent?

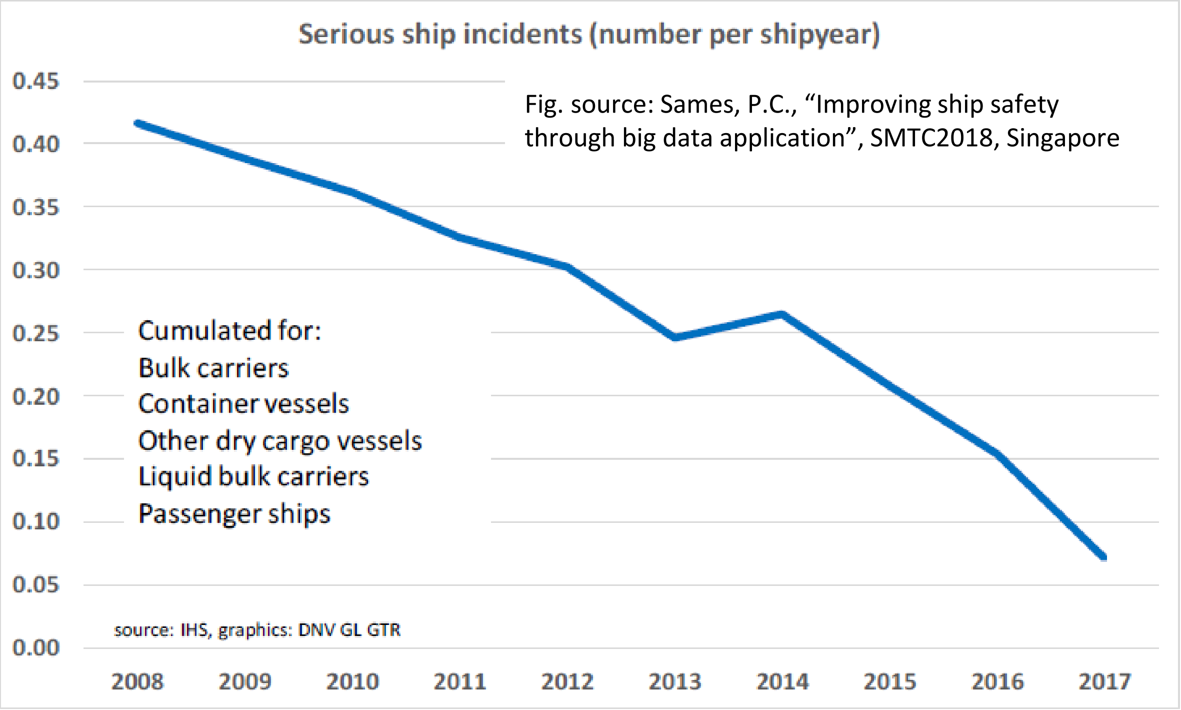


Fig. source: Sames, P.C., "Improving ship safety through big data application", SMTC2018, Singapore

source: IHS, graphics: DNV GL GTR

- What about learning systems?

Evolving Human-Machine Interfaces

AF 447

- Pitot tube obstructed by ice-crystals
- HMI issues
  - Conflicting / wrong / insufficient info
  - Crew reaction
  - Sidestick control design (no tactile feedback, pilot & co-pilot not linked)

Boeing 737 MAX (ET302 & Lion Air JT610)

- System design
  - Manoeuvring Characteristics Augmentation System
  - Angle of attack sensor system
  - Redundancy & cross-checking
- Crew training & procedures

ConOps – Risk assessment

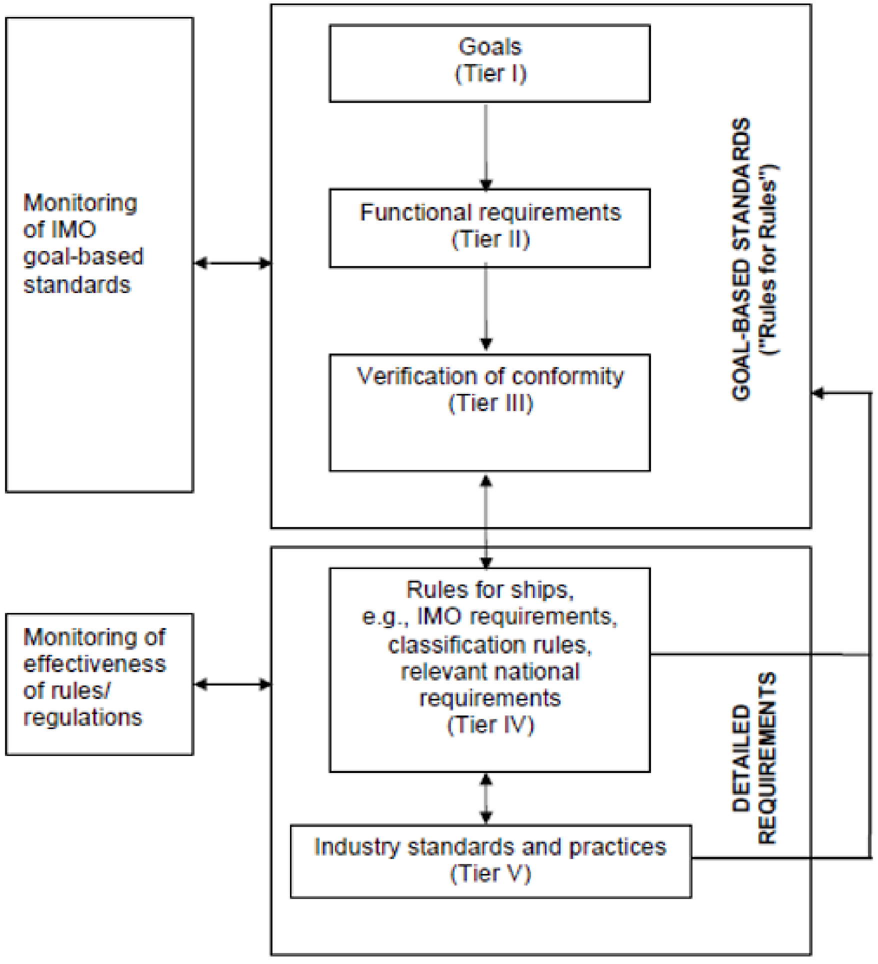
ConOps – Concept of Operations

- Origins: software engineering & information systems (ISO/IEC/IEEE 24765)
- To communicate quantitative & qualitative system characteristics
  - Statement of an organisation's assumptions or intent in regard to an operation or series of operations
- ConOps usually includes the following:
  - Goals and objectives of the system;
  - Strategies, tactics, policies, and constraints affecting the system;
  - Organizations, activities, and interactions among participants and stakeholders;
  - Clear statement of responsibilities and authorities delegated;
  - Specific operational processes for fielding the system;
  - Processes for initiating, developing, maintaining, and retiring the system

Risk Assessment – Safety Assurance

- Integrate a variety of current and new methods for safety assurance, depending on need and system specifications
- To include:
  - Risk-based methods (Risk-based design) – **issue with lack of data**
  - Paradigm shift from R = P x C to expressions of risk involving uncertainty & potential consequences
    - **Qualitative**
    - **"Unknown unknowns"**
  - System theoretic process analysis (STPA)
  - Goal-Based Standards, FSA, Safety case approach

Relevance of IMO GBS


Monitoring of IMO goal-based standards
Goals (Tier I)
Functional requirements (Tier II)
Verification of conformity (Tier III)
GOAL-BASED STANDARDS ("Rules for Rules")
Monitoring of effectiveness of rules/ regulations
Rules for ships, e.g., IMO requirements, classification rules, relevant national requirements (Tier IV)
Industry standards and practices (Tier V)
DETAILED REQUIREMENTS

GOAL-BASED STANDARDS FRAMEWORK

Source: IMO. 2010. "Adoption of the International Goal-Based Ship Construction Standards for Bulk Carriers and Oil Tankers. Resolution MSC.287(87)." London

Tier I – Goals: High-level objectives to be met.

Tier II – Functional requirements: Criteria to be satisfied in order to conform to the goals.

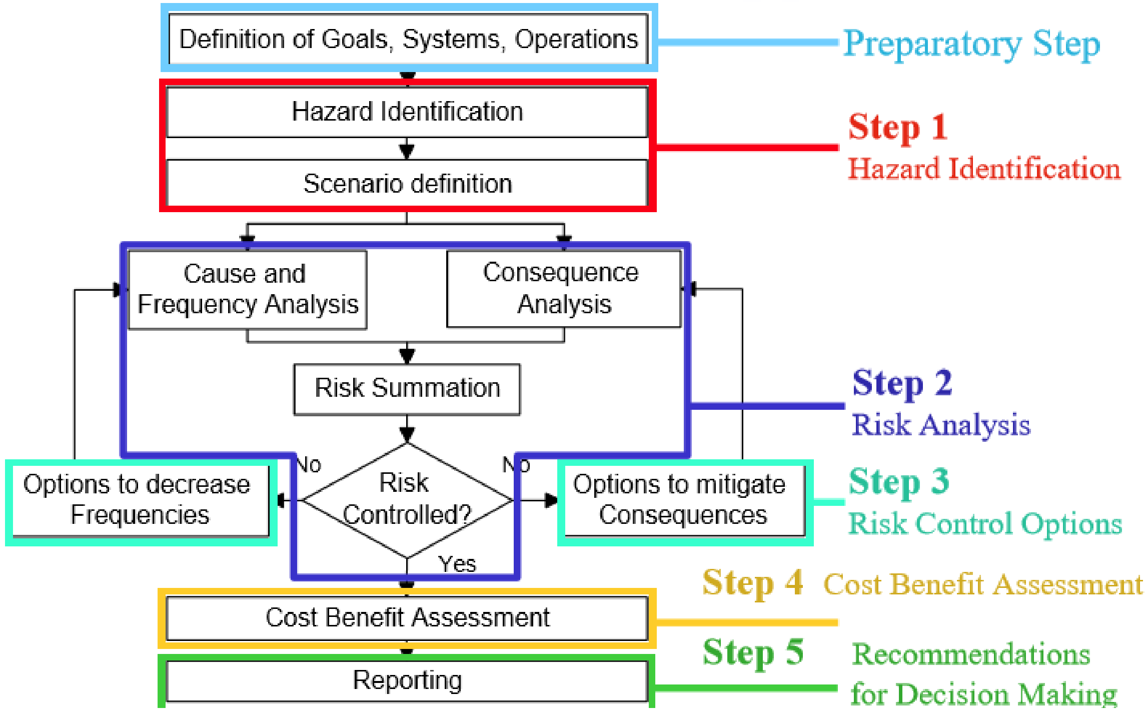
Tier III – Verification of conformity: Procedures for verifying that the rules and regulations for ship design and construction conform to the goals and functional requirements.

Tier IV – Rules and regulations for ship design and construction: Detailed requirements developed by IMO, national Administrations and/or recognized organizations and applied by national Administrations and/or recognized organizations acting on their behalf to the design and construction of a ship in order to conform to the goals and functional requirements.

Tier V – Industry practices and standards: Industry standards, codes of practice and safety and quality systems for shipbuilding, ship operation, maintenance, training, manning, etc., which may be incorporated into, or referenced in, the rules and regulations for the design and construction of a ship.

Source: IMO website

Formal Safety Assessment



Definition of Goals, Systems, Operations

Preparatory Step

Hazard Identification

Scenario definition

Step 1
Hazard Identification

Cause and Frequency Analysis

Consequence Analysis

Risk Summation

Step 2
Risk Analysis

Options to decrease Frequencies

No

Risk Controlled?

No

Yes

Options to mitigate Consequences

Step 3
Risk Control Options

Step 4 Cost Benefit Assessment

Cost Benefit Assessment

Step 5 Recommendations for Decision Making

Reporting

FSA – Supportive **tool for rule-making** at IMO providing a proactive and holistic risk-based approach comprising technical, human and operational aspects → systematic, objective, comprehensive, auditable, documented

Source: IMO: "Revised Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process", MSC-MEPC.2/Circ.12/Rev.2, 9 April 2018.

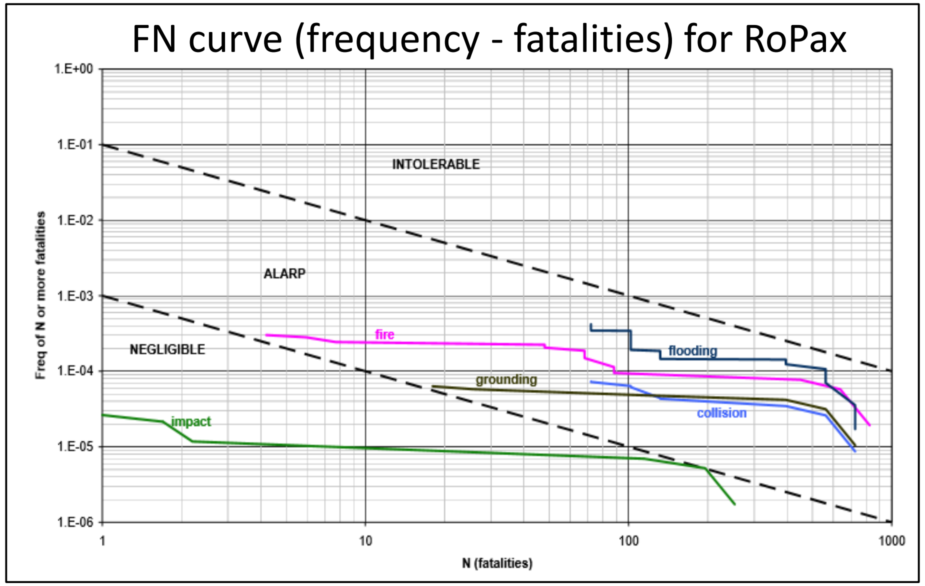


Fig. source: "FSA – RoPax ships", MSC 85/INF.3, 21 July 2008

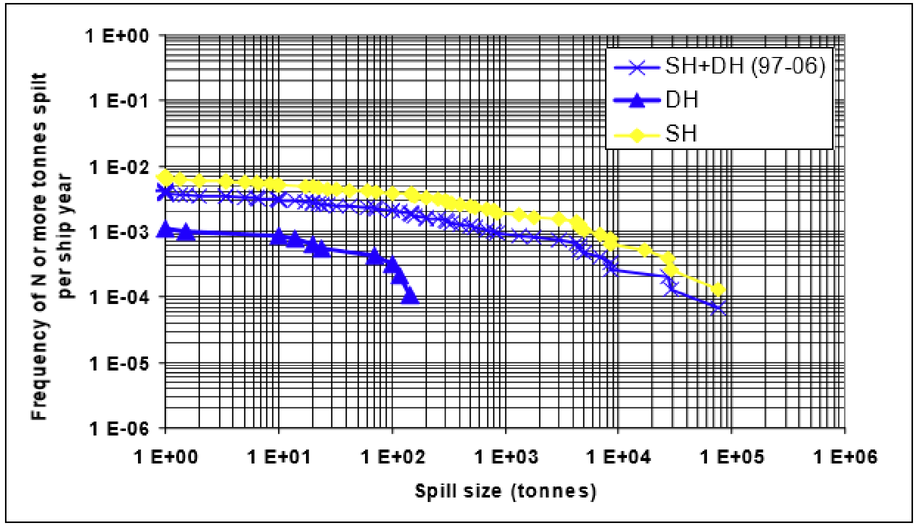
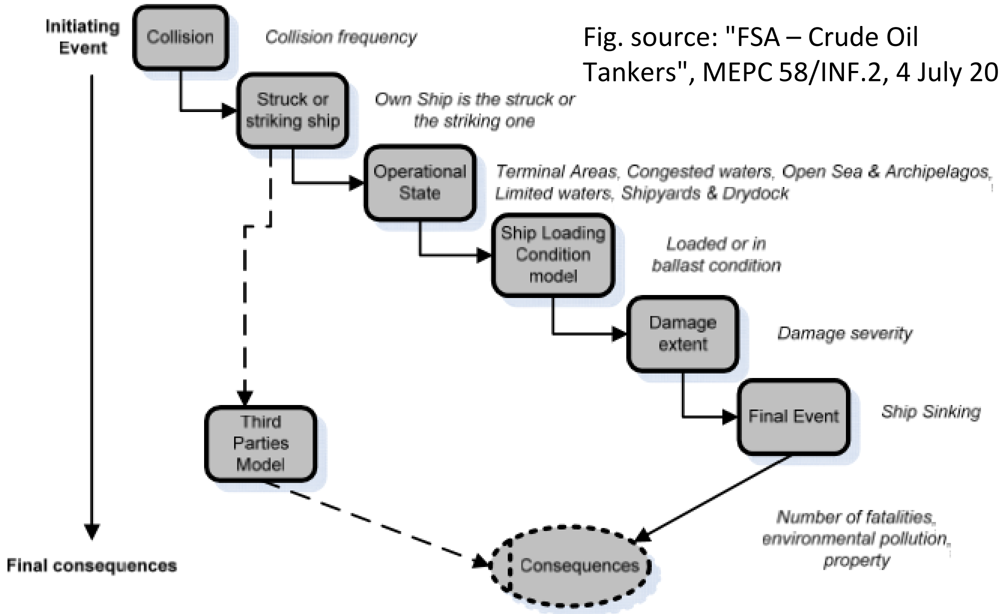


Fig. source: "FSA – Crude Oil Tankers", MEPC 58/INF.2, 4 July 2008

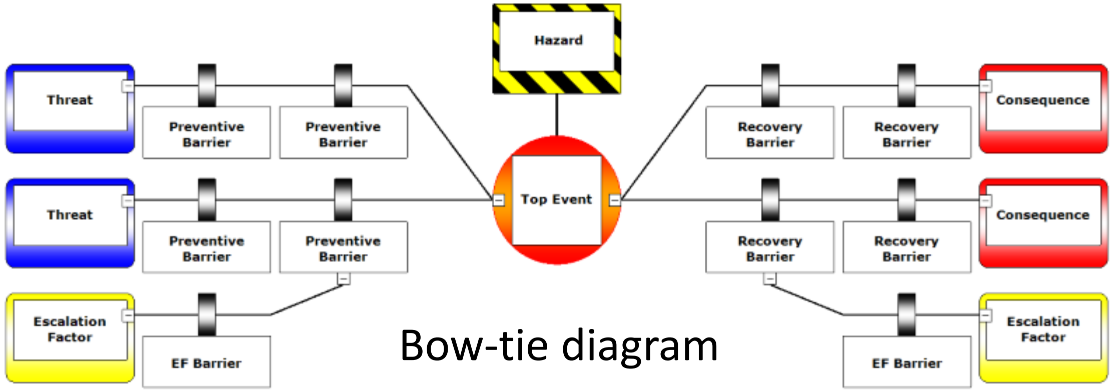
Formal Safety Assessment & Risk-based methods



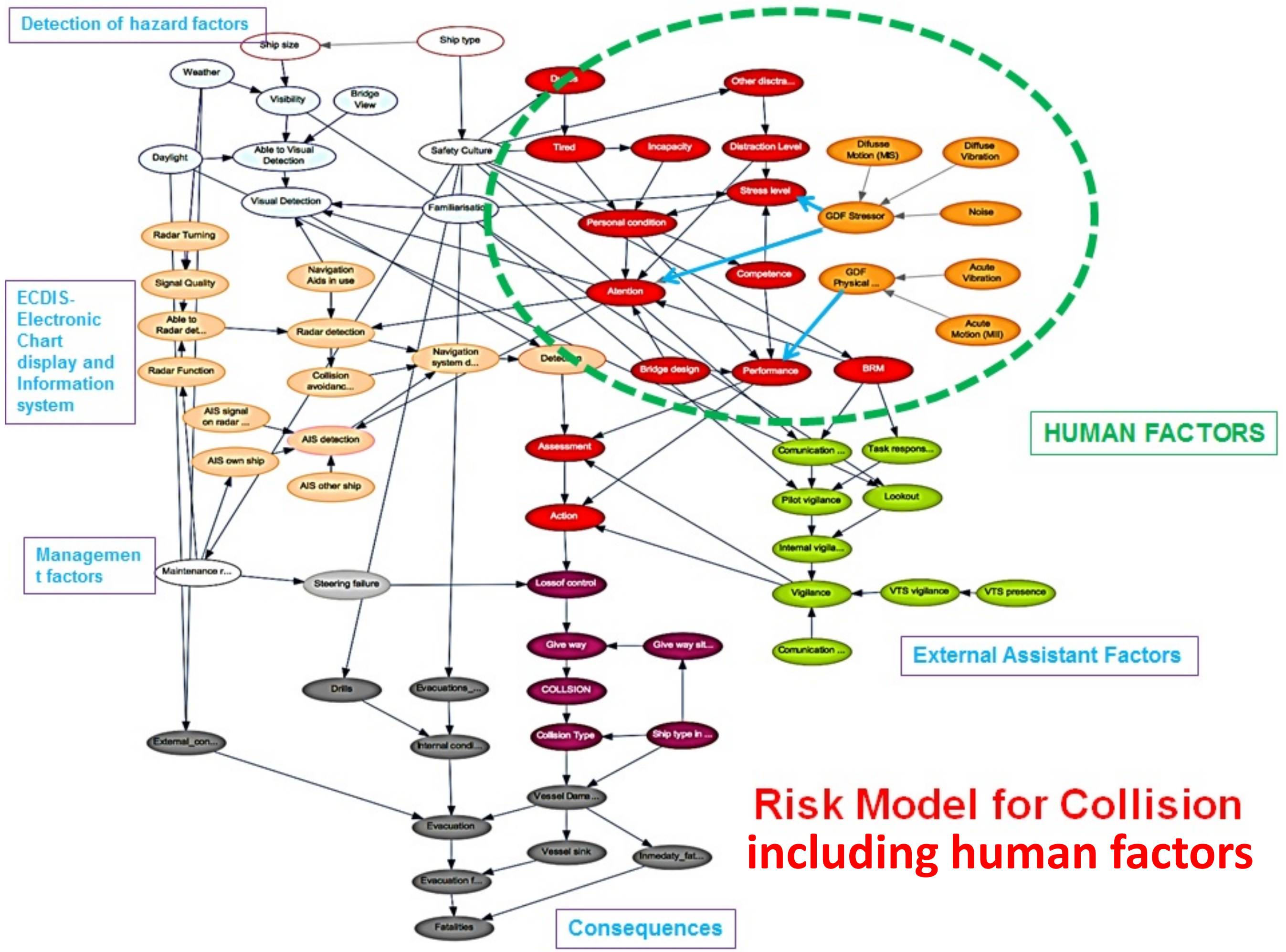
Initiating Event
Collision
Collision frequency
Struck or striking ship
Own Ship is the struck or the striking one
Operational State
Terminal Areas, Congested waters, Open Sea & Archipelagos, Limited waters, Shipyards & Drydock
Ship Loading Condition model
Loaded or in ballast condition
Damage extent
Damage severity
Final Event
Ship Sinking
Third Parties Model
Consequences
Number of fatalities, environmental pollution, property
Final consequences

Fig. source: "FSA – Crude Oil Tankers", MEPC 58/INF.2, 4 July 2008

Figure 16: Event sequence in collision risk model of an Oil Tanker



Bow-tie diagram



Risk Model for Collision including human factors

Fig. source: Endrina, N., Konovessis, D., Sourina, O., Krishnan, G.: "Influence of ship design and operational factors on human performance and evaluation of effects and sensitivity using risk models", Ocean Engineering, 184, pp. 143-158.

Potential methods: STAMP / STPA

STAMP (Systems-Theoretic Accident Model and Processes)

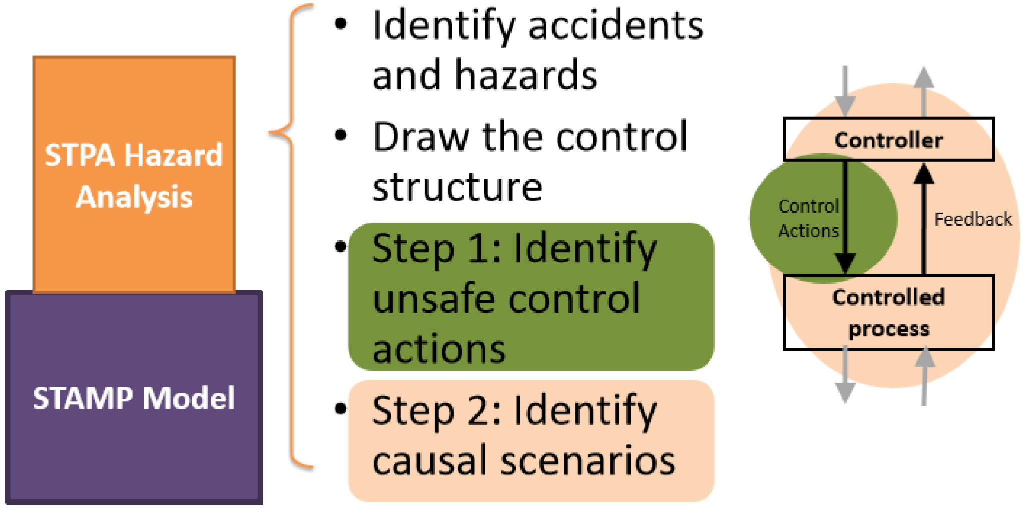
- is an accident causality model based on systems theory and systems thinking
- integrates into engineering analysis causal factors such as software, human decision-making and human factors, new technology, social and organizational design, and safety culture,
- becoming ever more threatening in our increasingly complex systems

STPA (Systems-Theoretic Process Analysis)

- Powerful hazard analysis technique based on STAMP
- CAST (Causal Analysis based on STAMP) is the equivalent for accident and incident analysis.
- Ongoing developments aim at extending the application field of STPA to include security.

STPA

(System-Theoretic Process Analysis)



STPA Hazard Analysis

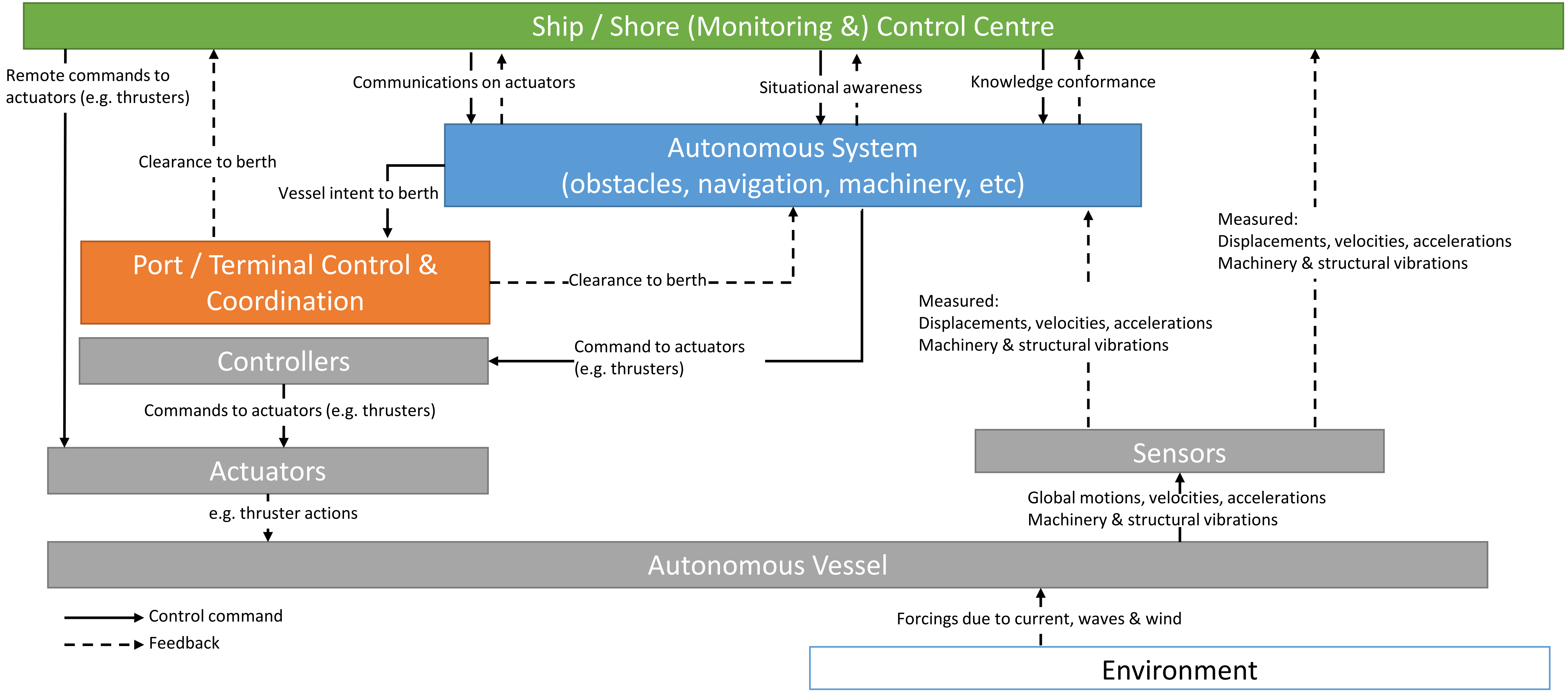
STAMP Model

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

Can capture requirements flaws, software errors, human errors

Fig. source: Leveson, N. G.: "Engineering a Safer World", MIT Press, 2011

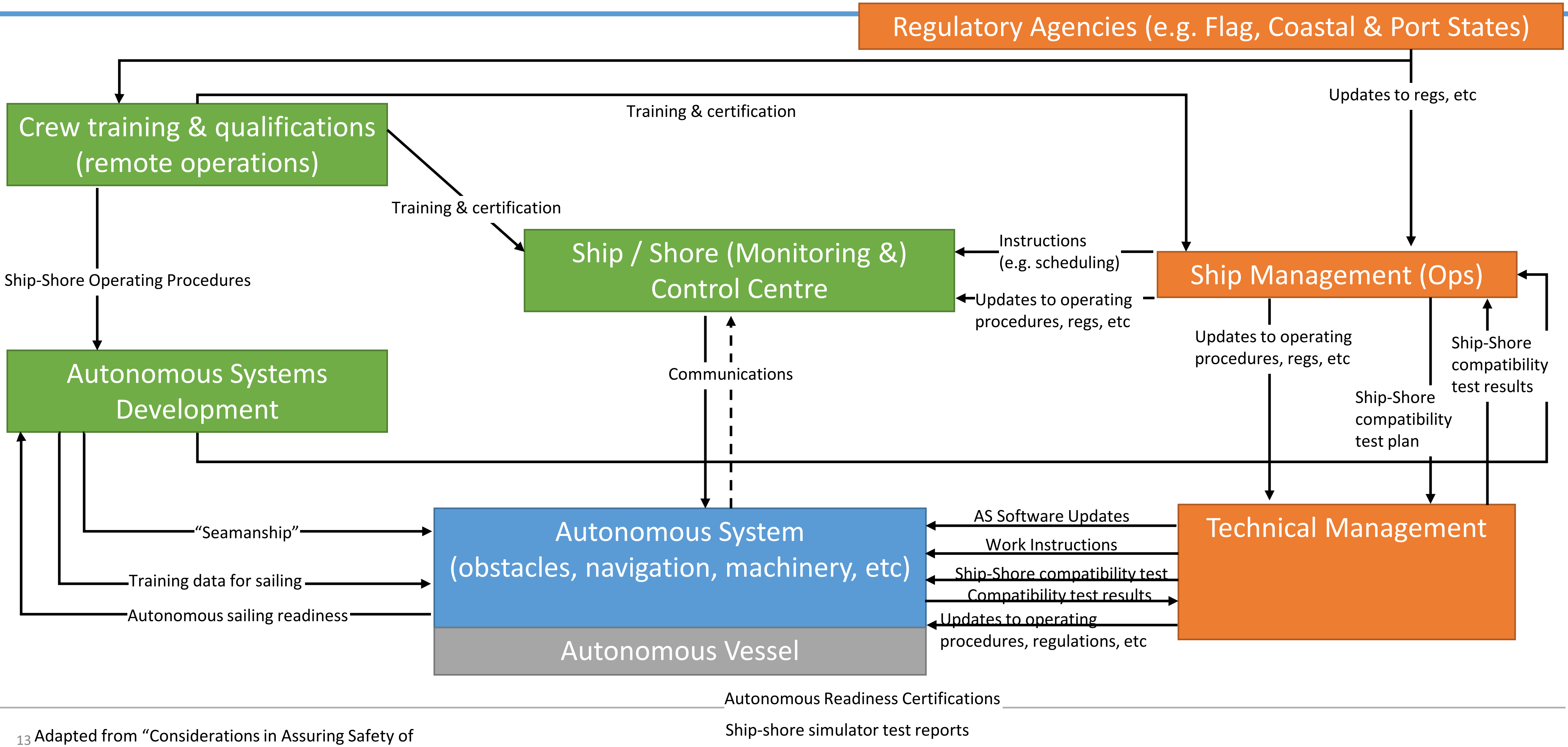
STPA: Example (Vessel System)



Ship / Shore (Monitoring &) Control Centre
Remote commands to actuators (e.g. thrusters)
Communications on actuators
Situational awareness
Knowledge conformance
Clearance to berth
Vessel intent to berth
Autonomous System (obstacles, navigation, machinery, etc)
Measured: Displacements, velocities, accelerations Machinery & structural vibrations
Port / Terminal Control & Coordination
Clearance to berth
Measured: Displacements, velocities, accelerations Machinery & structural vibrations
Controllers
Command to actuators (e.g. thrusters)
Commands to actuators (e.g. thrusters)
Sensors
Actuators
Global motions, velocities, accelerations Machinery & structural vibrations
e.g. thruster actions
Autonomous Vessel
Control command
Feedback
Forcings due to current, waves & wind
Environment

Adapted from "Considerations in Assuring Safety of Increasingly Autonomous Systems , NASA/CR-2018-220080"

STPA: Example (Vessel Management Level)


Regulatory Agencies (e.g. Flag, Coastal & Port States)
Updates to regs, etc
Training & certification
Crew training & qualifications (remote operations)
Training & certification
Ship / Shore (Monitoring &) Control Centre
Instructions (e.g. scheduling)
Updates to operating procedures, regs, etc
Ship Management (Ops)
Ship-Shore Operating Procedures
Autonomous Systems Development
Communications
Updates to operating procedures, regs, etc
Ship-Shore compatibility test results
Ship-Shore compatibility test plan
"Seamanship"
Training data for sailing
Autonomous sailing readiness
Autonomous System (obstacles, navigation, machinery, etc)
Autonomous Vessel
AS Software Updates
Work Instructions
Ship-Shore compatibility test
Compatibility test results
Updates to operating procedures, regulations, etc
Technical Management
Autonomous Readiness Certifications
Ship-shore simulator test reports

Adapted from "Considerations in Assuring Safety of Increasingly Autonomous Systems , NASA/CR-2018-220080"

Possible Future Work

- STAMP / STPA
- Explainable & Inspectable A.I.
- Human-in-the-loop (HITL)
  - Testing Human-Machine teams
  - Cross-understanding
- Test until safe recovery vs Test until failure?
  - Able to recover past initial failures to safe state: equivalent to human’s ability to react & respond
- Beyond reliability of components: Global hydrodynamics coupled with autonomous systems

*Considerations in Assuring Safety of Increasingly Autonomous Systems , NASA/CR-2018-220080

DNV·GL SiT SINGAPORE INSTITUTE OF TECHNOLOGY TCOMS

Thank you