Aalto University
School of Engineering

MEC-E2009 - Marine Risks and Safety

L3
System Safety Engineering and STAMP

Osiris A. Valdez Banda
Assistant Professor
Research Group on Safe and Efficient Marine and Ship Systems

Learning logs L2

Feedback

Learning logs L2

Fast quiz L2

Min	Max	Grade
0	50	0
50	60	1
60	70	2
70	80	3
80	90	4
90	100	5

L2: Intended Learning Outcome (ILO)

ILO 1

The students learn and reflect on existing accident causality models and their differences.

ILO 2

The student learn and understand the foundations and objectives of System-Theoretic Accident Model Processes (STAMP) and two of its family tools (STPA and the Safety Intent Specification)

Why another way to analyse risk and safety

Background

Accident Causality Models

- Underlie all our efforts to engineer for safety
- Explain why accidents occur
- Determine the way we prevent and investigate accidents
- Imposes patterns on accidents
- Those models are never entirely correct but some of them are useful

Background

How Accident Causality Models traditionally cope with complexity?

- Analytic Reduction
- Statistics
- Systems Theory

Background

Analytic Reduction approach to safety

- Divide system into distinct parts for analysis
  - Physical aspects →Separate physical components or functions
  - Behavior →Events over time

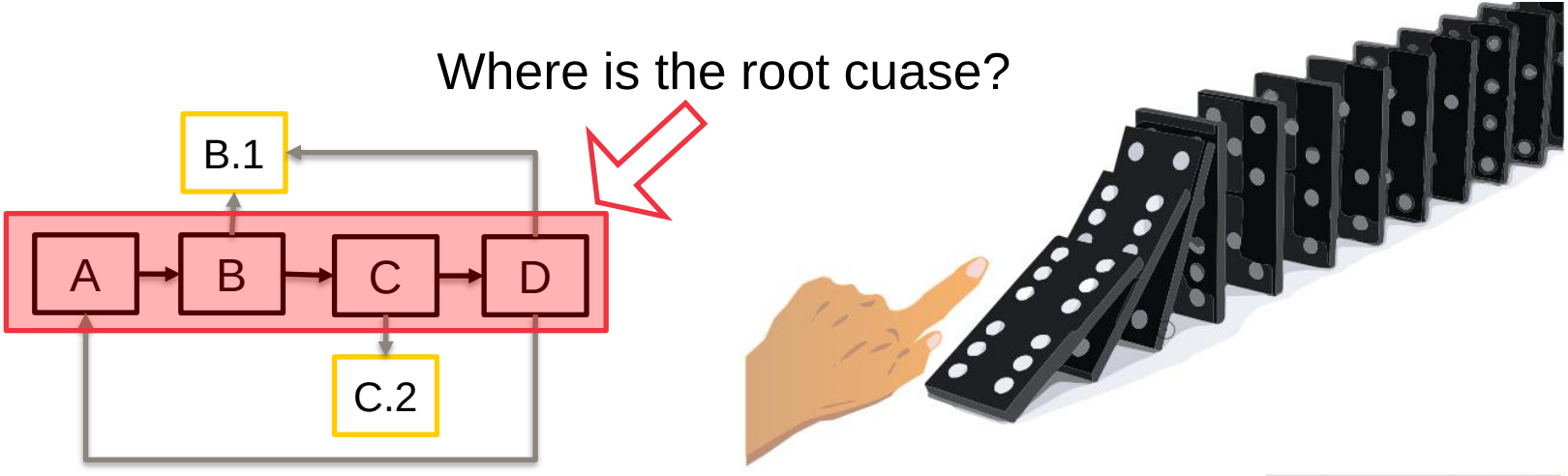
- Examine parts separately and later combine analysis results

- Assumes such separation does not distort phenomenon
  - ✓ Each component or subsystem operates independently
  - ✓ Components act the same when examined singly as when playing their part in the whole

- Events not subject to feedback loops and non-linear interactions

Background

Examples

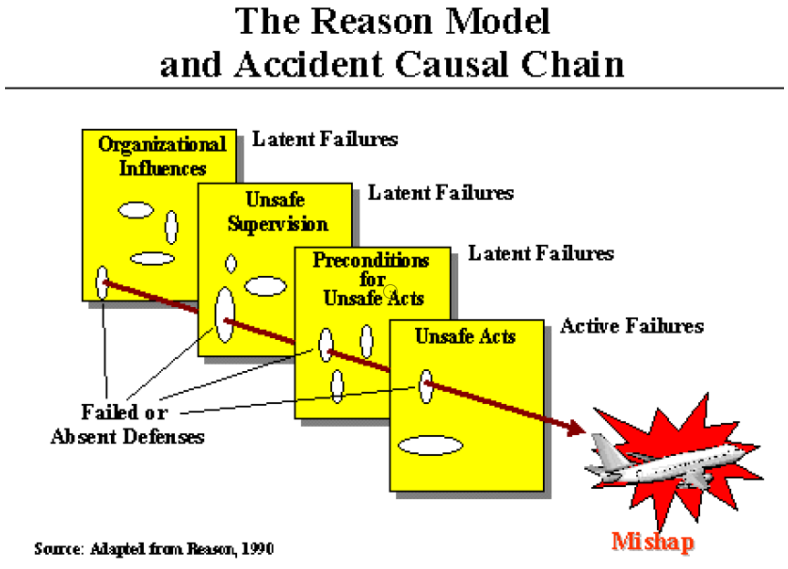


Domino “Chain of events” Model

Background

Examples

- The holes represent failed or absent barriers or defenses (of a system)
- Ignores common cause failures of defenses (systemic accident factors)
- Does not include migration to states of high risk
- Assumes accidents are random events coming together accidentally
- Assumes some (linear) causality or precedence in the cheese slices (and holes)
- Just a chain of events, no explanation of "why" events occurred



Swiss Cheese model

Background

Analytic Reduction does not Handle

- Component interaction accidents
- Systemic factors (affecting all components and barriers)
- Software and software requirements errors
- Human behavior (in a non-superficial way)
- System design errors
- Indirect or non-linear interactions and complexity
- Migration of systems toward greater risk over time (e.g., in search for greater efficiency and productivity)

Background

Statistics

- Useful to understand a general safety outcome
- Are the basis for many of the safety analysis made in different industries (heavily used in maritime safety analysis)
- Limited to the information available in past events
- Provide a numerical outcome based on many qualitative elements integrated in the system
- Approach that tends to transform outcome into probabilities, provoking an erroneous focus just in numbers
- Complex to use for the analysis of the system interactions.

Background

Systems Theory

- ✓ Developed for systems that are
  - Too complex for complete analysis
    - * Separation into (interacting) subsystems distorts the results
    - * The most important properties are emergent
  - Too organized for statistics
    - * Too much underlying structure that distorts the statistics
    - * New technology and designs have no historical information
- ✓ Focuses on systems taken as a whole, not on parts taken separately
- ✓ Emergent properties
  - Some properties can only be treated adequately in their entirety, taking into account all social and technical aspects
  - These properties arise from relationships among the parts of the system

Background

In real life, any system managing the safety of e.g. a ship and its interconnection with other internal (management, operation, technical elements) and external system components (other stakeholders involved in the management of safety) are too complex to analyze effectively without a systematic and systemic view and clear understanding of the component interaction in the system.

So, what approach could be used?

System-Theoretic Accident Model Processes

(STAMP)

Aalto University
School of Engineering

Accident Causality Traditional View vs STAMP view

Traditional:

- Accidents are chains of directly related events
- Safety = management of failures
- Direct causality

STAMP:

- Accidents involved complex dynamic processes
- Safety = Dynamic control problem
- Direct and indirect causality

Applying STAMP

Accidents involved a complex, dynamic “process”

- Not simply chains of failure events
- Arise in interactions among humans, machines and the environment

Treat safety as a dynamic control problem

- Safety requires enforcing a set of constraints on system behavior
- Accidents occur when interactions among system components violate those constraints
- Safety becomes a control problem rather than just a reliability problem

STAMP is composed by 3 basic concepts

1. Safety constraints
2. Hierarchical safety control structures
3. Process models

1. Safety contraints

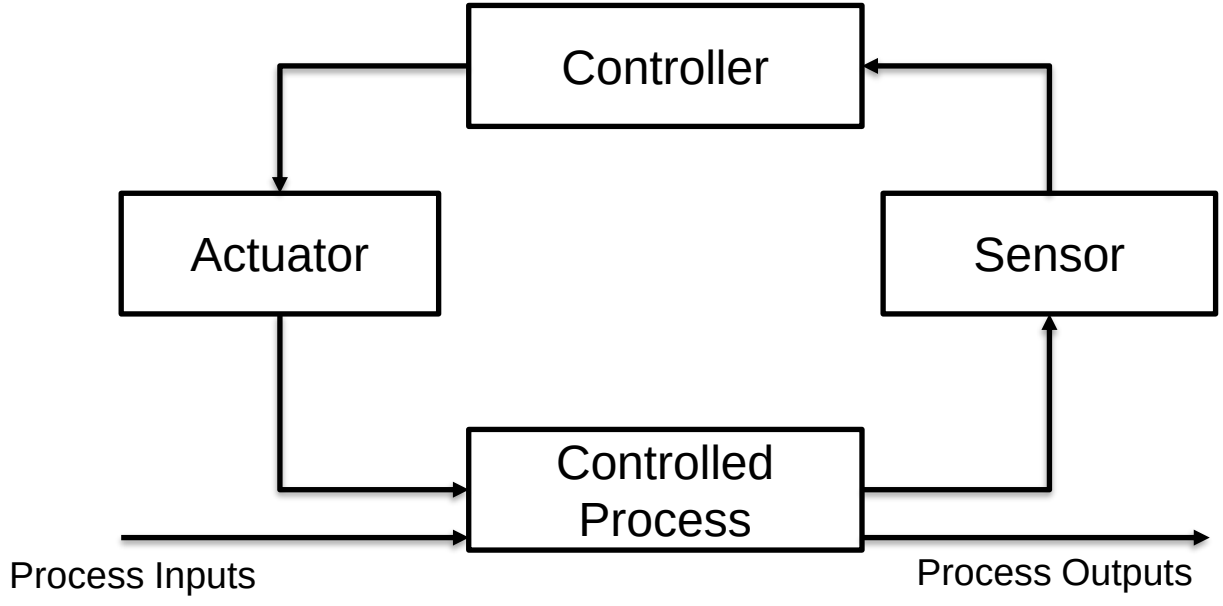
Safety as a Dynamic Control Problem

Events are the result of the inadequate control

Result from lack of enforcement of safety constraints in system design and operations

A change in emphasis:

Safety constraints to prevent accidents



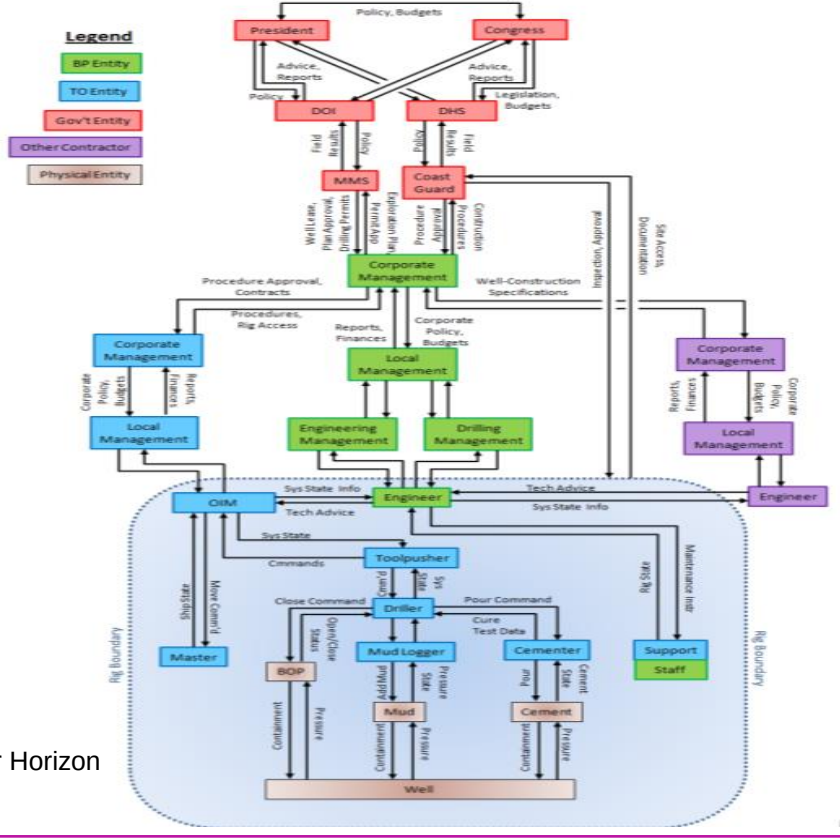
Control Feedback Loop

2. Hierarchical safety control structures

A hierarchical safety control structure is an instance of the more general system theory concept of hierarchical control structure. The goal of the safety control structure (sometimes called the safety management system) is **to enforce safety constraints and therefore eliminate or reduce losses**.

Example of hierarchical sociotechnical control

Part of defining the safety control structure is a specification of the expectations, responsibilities, authority, and accountability with respect to enforcing safety constraints of every component at every level.

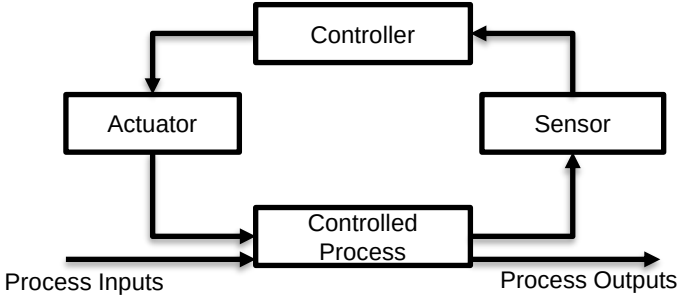


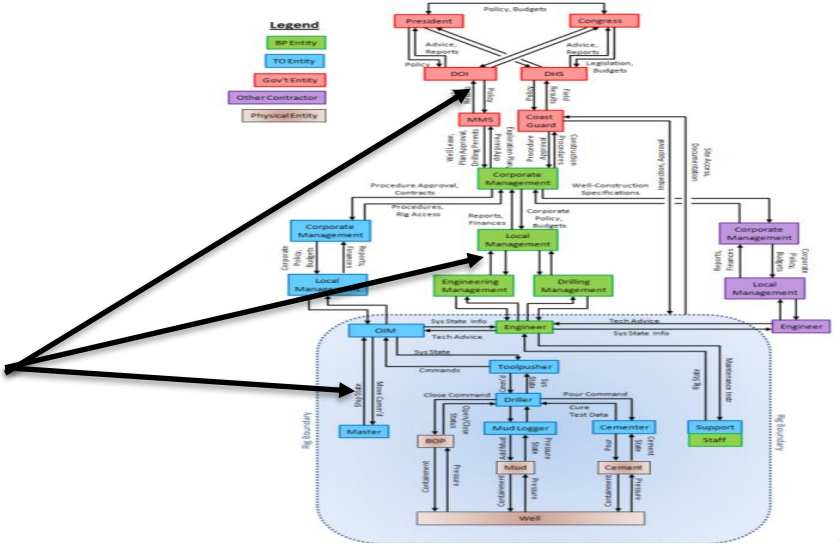
The safety control structure over the Macondo well during the Deepwater Horizon accident as Presented in Leveson 2017

Leveson, N. 2017. STPA-Primer . MIT press 2017 Version 1.

3. Process models

Control loops exist between every level of the safety control structure, even those at the management and organizational level. Each component in the hierarchical safety control structure has responsibilities for enforcing safety constraints appropriate for that component.





Summary:

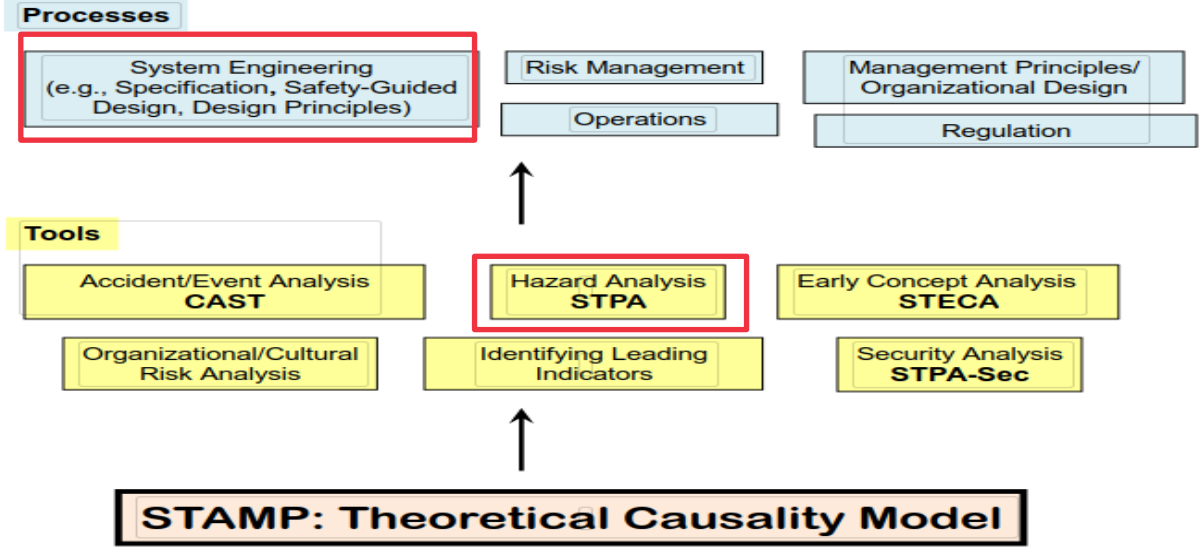
- In STAMP, accidents involve a complex and dynamic process. They are not simply chains of component failure events. Safety is treated as a dynamic control problem, rather than a component reliability problem.

  “In the example of the hierarchical control structure: the problem at the Deepwater Horizon fire and oil spill was a lack of control over the pressure in the well. However, this is linked to lack of controls in the different components managing the safety of the operations.

- So, with the STAMP approach we can detect system design errors, software requirements flaws, mistakes in human decision making, migration of the overall system toward states of higher risk, etc.”

Summary:

- STAMP **is only** an accident causation model, it is not itself an engineering technique.
- However, by using STAMP as a theoretical foundation, new **tools and processes** can be constructed.



Group Discussion

STAMP Safety Intent Specification

AIM of STAMP Safety Intent Specification

An intent specification aims at assisting humans in dealing with complexity. It differs from the specification based on standard regulations in its structure but not in its content, the main difference is that intent specifications contain more detailed information.

The intent specification is organized into different hierarchy levels which provide information about the reasons behind the design decisions for assembling the management of organizational safety.

Structure of the safety intent specification

	Environment	Operator	System and components	Verification and validation
Level 0: Program management	Management plans, safety plan, safety management procedures and safety plans			
Level 1: System purpose	Assumptions and constraints	Responsibilities Requirements	Goals, requirements, design, constraints and limitations	Preliminary Hazard analysis
Level 2: System principles	External interfaces	Task analysis and allocation, Controls and Displays	Logic principles, functional decomposition and allocation	Validation plan and System Hazard analysis
Level 3: System architecture	Environment models	Operator Task models and HCI models	Blackbox functional models and Interface specifications	Analysis plans and results, Subsystem Hazard analysis
Level 4: Design representation		Human – Computer Interface Design	Software and hardware design aspects	Test plans and results
Level 5: Physical representation		Guided User Interface design, physical control design	Software code, hardware assembly instructions	Test plans and results
Level 6: System operations	Audit procedures	Operator manuals, Maintenance and training materials	Error reports, and change request.	**Performance monitoring (KPIS)**

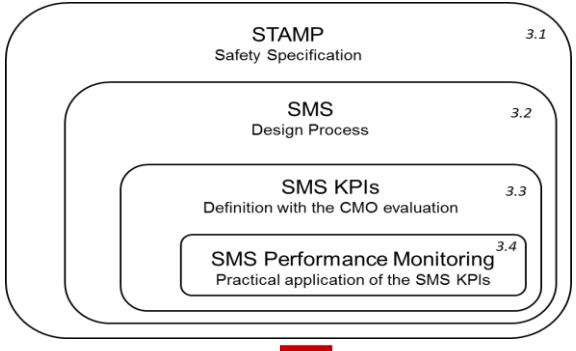
The safety intent specification (adapted from Leveson 2011)

When to use the Safety Intent Specification

- For designing the structure of a new safety management system
- For evaluating the functioning of an operating safety management system
- For applying an evaluation of certain aspects influencing the management of safety in the organization or a particular operation
  - Applying only a certain level for analysis
  - Executing a part of a systematic hazard analysis
  - Analysing the outcome of the operations

Example of implementing the Safety Intent Specification

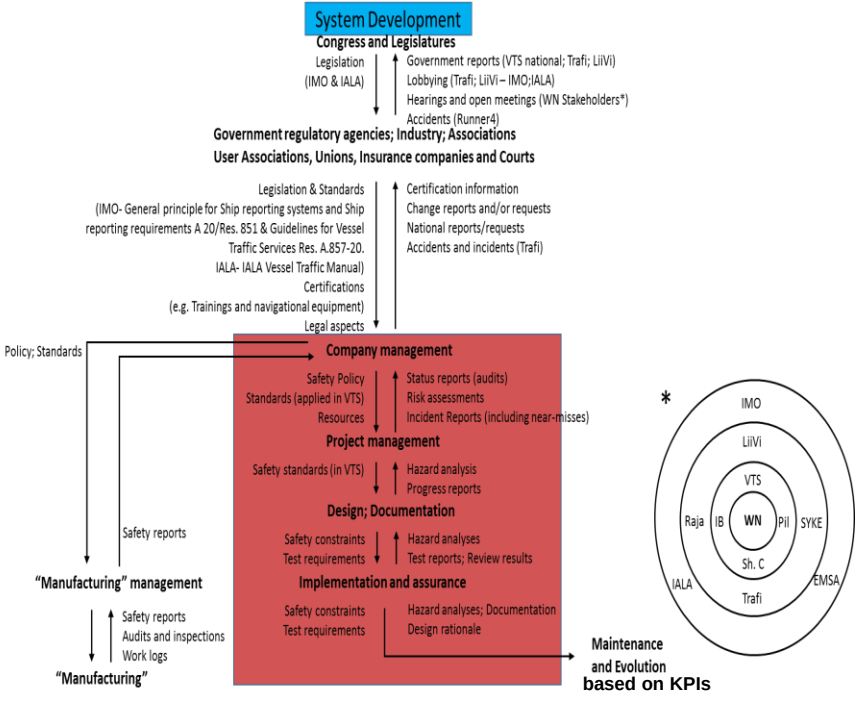
Implementing the Safety Intent Specification (CASE study)



	Environment	Operator	System and components	Verification and validation
Level 0: Program management	Management plans, safety plan, safety management procedures and safety plans			
Level 1: System purpose	Assumptions and constraints	Responsibilities Requirements	Goals, requirements, design, constraints and limitations	Preliminary Hazard analysis
Level 2: System principles	External interfaces	Task analysis and allocation, Controls and Displays	Logic principles, functional decomposition and allocation	Validation plan and System Hazard analysis
Level 3: System architecture	Environment models	Operator Task models and HCI models	Blackbox functional models and Interface specifications	Analysis plans and results, Subsystem Hazard analysis
Level 4: Design representation		Human – Computer Interface Design	Software and hardware design aspects	Test plans and results
Level 5: Physical representation		Guided User Interface design, physical control design	Software code, hardware assembly instructions	Test plans and results
Level 6: System operations	Audit procedures	Operator manuals, Maintenance and training materials	Error reports, and change request.	**Performance monitoring (KPIS)**

Safety Intent Specification

VTS Finland

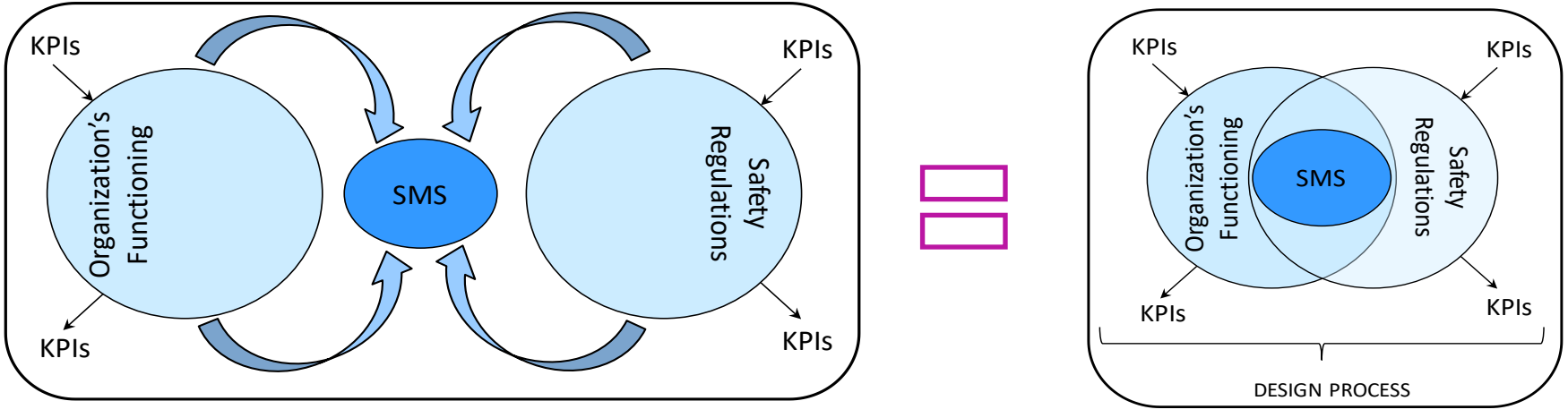


VTS Socio-technical structure

Valdez Banda, O. A. & Goerlandt, F. (2018). A STAMP-based approach for designing maritime safety management systems. Safety Science, 109, 109-129.

Safety management systems

A SMS is the commonly utilized vehicle to achieve the safety objectives of an organization. SMS must effectively understand the internal functioning of the organization while also implementing and complying with safety regulations



Elements influencing and interacting in the function of SMS (Valdez Banda et al. 2018)

Proposed process for designing SMS

Level	Task
0	Review of the current practices for managing the function of the organization
1	Define system goals and constraints • Define accidents • Hazard identification • Preliminary hazard analysis • Environmental assumptions • Initial restrictions of the SMS • SMS requirements • Link between the requirements and detected hazards • High-level safety constraints of the SMS
2	Integrated principles for the function of the SMS under design • Interface • Hazard analysis and validation of the requirements
3 – 5*	Architectural design and functional allocation • Mapping of the elements in the SMS System design and physical representation. • Assessing of the SMS design and physical representation
6	Review of the actual performance of the designed SMS • Elaboration of auditing procedure • Review of personnel skills (training provision) and safety management (internal audit) • Definition of the KPIs for the SMS • Monitoring the performance of the SMS

Case study: VTS Finland

VTS Finland provides services for monitoring, communicating and reporting any event or issue related to the maritime traffic.

VTS areas:

- Bothnia VTS
- West Coast VTS
- Archipelago VTS
- Hanko VTS
- Helsinki VTS
- Kotka VTS
- Saima VTS

VTS centres:

- Gulf of Finland VTS
- Western Finland VTS
- Saima VTS

VTS Finland (services provided)

Information: traffic conditions in the areas and the condition of the aids to navigation and channels.

Navigational assistance: the vessel's position and bearings/courses over ground. It is provided at open sea, and from the open sea to the vicinity of pilot boarding places and also outer anchorages. It is only advisory and normative, the *master* is the final responsible for manoeuvring the vessel.

Traffic organization: this is given to prevent dangerous meeting, crossing and overtaking situations and congestion. For this, VTS separates the traffic in terms of time or distance according to the situation and circumstances.

Output (Level 0)

Review of the current practices for managing the function of the organization:

- The structured VTS Finland Quality Management Systems is the basis for the designing of the SMS.

Process	IALA Guideline
Routine processes	
A. Identification of ships entering the area	1056; 1111; 1089; 1105; 1083; 1102;1071; V-127; V-103
B. Identification of ships leaving port	1089; 1083; 1102; 1071; V-127
C. Provision of VTS *The process is activated when the process A or B started*	1089; V-127
D. Gulf of Finland Reporting System (GOFREP) *It includes the reporting of deviations*	1018; V-127

Output (Level 1)

18 main accidents

Accident type	Accident	Navigational season
Internal	1. Fire on the VTS centre	Both seasons
	2. Blackout in the VTS centre	Both seasons
External	3. Collision ship-to-ship 3.1 In meeting 3.2 Passing 3.3 Crossing 3.4 In pilot assistance.	Both seasons
	4. Collision with a fixed object	Both seasons

26 identified hazards

Hazard	Accident
A.1 Electrical equipment without proper maintenance A.2 Flammable material no properly controlled A.3 Lighting during storm affecting electrical equipment A.4 Fire in neighbouring building and/or office	1
B.1 Power grid failure B.2 Electrical equipment without proper maintenance	2
C.1 Radar equipment without proper maintenance C.2 Image system (AIS) outdated and/or without proper maintenance C.3 Communication equipment (radio, telephone, and IT) without proper maintenance C.4 Weather causing failures (lighting storms, winter storms, heavy rain, strong winds..)	F1

Preliminary Hazard analysis

Hazard	Severity				Likelihood
	H	T	E	P	
A.1	3	1	2	4	Low
A.2	3	1	2	4	Low
A.3	2	1	2	3	Low
A.4	3	1	2	3	Low
B.1	1	1	1	2	Medium
B.2	2	1	1	2	Low
C.1	1	3	1	2	Low
C.2	1	3	1	1	Low
C.3	1	2	1	1	Low
C.4	1	2	1	2	Medium

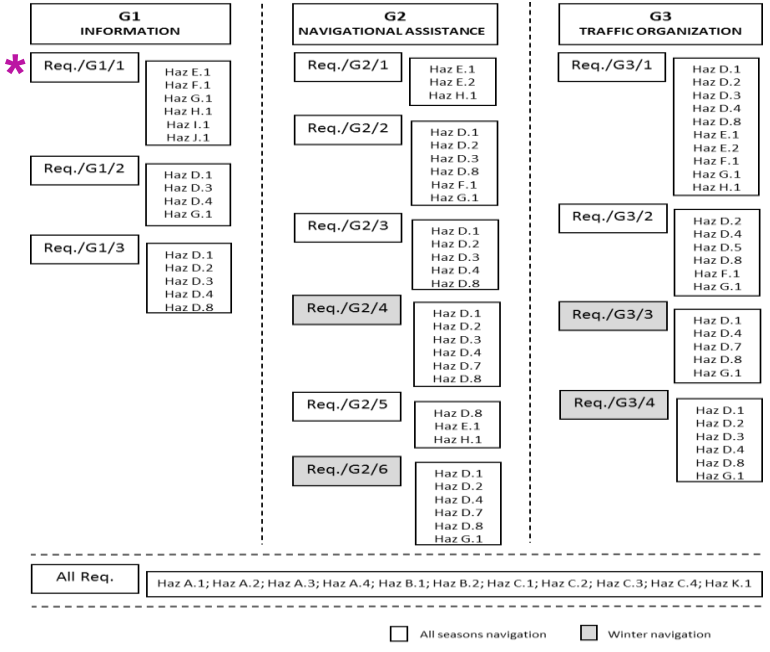
Severity Level	H Human	T Traffic operations	E Environment	P Property
4	Loos of life	Traffic operations discontinued	Catastrophic affectations to the environment	VTS centre/ ship loss
3	Severe injury or illness	Major affectations to the operations	Major affectations to the environment	VTS centre/ ship major damage
2	Minor injury or illness	Minor affectations to the operations	Minor affectations to the environment	VTS centre/ ship minor damage
1	Insignificant injury or illness	Insignificant affectations to the operations	Insignificant affectations to the environment	VTS centre/ ship insignificant damage

Output (Level 1)

Assumptions and constraints

Hazard D.2. VTS provide inappropriate navigational assistance to the vessels in the area.	
Assumption	Safety Constraints (SC)
EA/D.2/1 (List of information) EA/D.2/2 (Communication restrictions) EA/D.2/3 (International guidelines) EA/D.2/4 (Training)	SC. The IALA guidelines and recommendations are implemented in the functioning of all the VTS centres. This includes: • Acquisition of appropriate technology to provide VTS all year around (including wintertime). • The cooperation with all relevant stakeholders in the provision of navigational assistance • The safety and business strategy targets stated by VTS Finland and Finnish maritime authorities SC. VTS Finland executes periodical reviews for the testing the skills of the personnel of the centres. SC. The operators are trained to be efficient when providing navigational assistance. Demanded basic training by IALA is provided to operators and supervisors. The training is strengthened by having exercises in simulated environments which are evaluated by training experts.

Requirements of the SMS



*	Req./G1/1	15 minutes before entering a VTS area, vessels must provide its basic information (vessel name, location, destination, intended route and vessel general condition) to VTS centre.

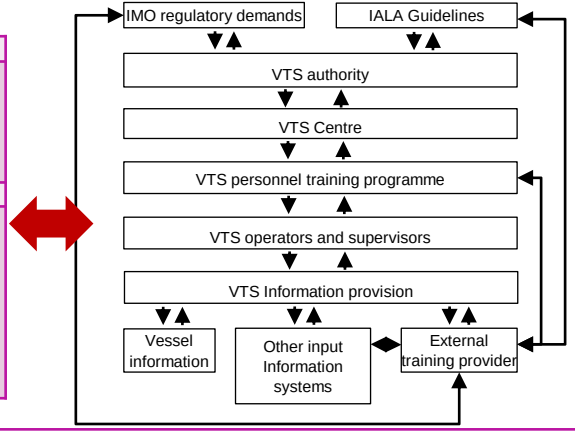
Output (Level 2)

Definition of the practical functioning of the requirements

Req./G2/2. A vessel approaching to a point of contingency must be informed about the situation and recommendations (guidance) should be provided.	
Interface	Radio is the most common mean used to inform about contingencies in the planned route. In case communication by radio is not possible, other alternatives must be used. The requirement could have connection with other organization such as: pilots, icebreakers, SAR services, shipping company and any organisation affected by the vessel logistics chain.
Controls and displays	Contingencies are reported by radio to VTS centres. This enables the marking and displaying of the areas of contingency within VTS monitoring system.
Logic principles	Once contingencies are reported, marked and displayed in the VTS monitoring system, VTS operators inform the potential risk to other vessels approaching the area and provide recommendations about how to proceed.

Re-defining the requirements

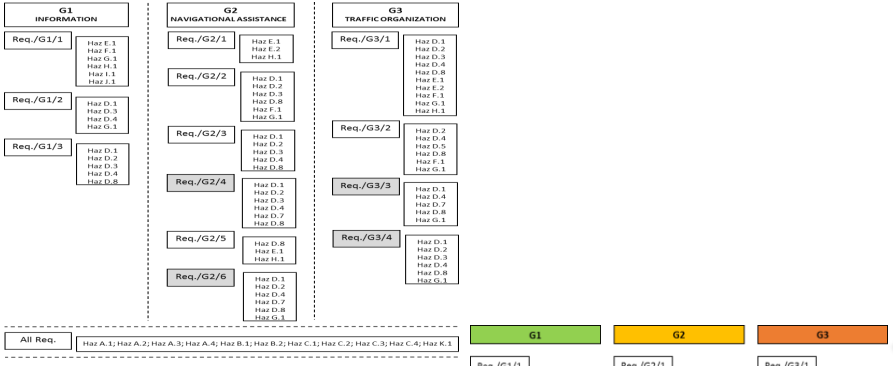
Detecting potentially Unsafe Controlled Actions (UCAs)
UCA 1. The training provided for VTS personnel does not consider the demands and guidelines of the existing normative. UCA 2. The training provided does not match the needs and common characteristics of an actual service provision. UCA 3. The training does not efficiently consider the actual scope and limitations on the provision of navigational assistance. UCA 4. The training does not efficiently consider the common input from relevant information systems such as pilots, icebreakers, SAR services
Redefine of the safety constraint
SC. The operators are trained to be efficient when navigational assistance. Demanded basic training by IALA is provided for operators and supervisors. The training is strengthened by having exercises in simulated environments which are evaluated by training experts. This includes: - Demanded basic training in IMO regulations (e.g. SCTW) and IALA guidelines are included in the training offered. - The training programme efficiently covers the specifications of the actual scope and limitation in the provision of navigational assistance by VTS Finland. - Trainers incorporate the actual characteristics on the exchange of information between VTS centres and vessels, including the understanding about the common conflicts during communication.



STPA process

Output (Level 3-5)

Analysis of the architectural design, system functional allocation and system physical representation



Requirements of the SMS to be evaluated and reviewed with the navigation monitoring system provider

1. General review of the requirements for the functioning of the SMS VTS Finland

Requirement	Hazards	Status and support evidence
Req./G1/1 Req./G1/2 Req./G1/3 Req./G2/1 Req./G2/2 Req./G2/3 Req./G2/4 Req./G2/5 Req./G2/6 Req./G3/1 Req./G3/3 Req./G3/4	A.1; A.3; B.1; B.2; C.1; C.2; C.4; D.1-4; E.1; E.2; F.1; G.1; H.1; K.1	Are the requirements informed and detailed explained to the provider? Are the assumptions and hazards explained and reviewed with the provider? - Documents of reference: Are the requirements fulfilled by the provider? - Exceptions: Are the general aspects of the monitoring system improved after reviewing the requirements with the provider? - Provide a documented action: Evaluation of Ergonomics

2. The VTS Finland monitoring system must follow the demands in international regulations which are adapted to the requirements.

Regulation	Req.	Condition evaluated
IALA Guideline 1056	Radar	Are the requirements of the regulation fulfilled?

Output (Level 6)

- A defined internal audit procedure for the SMS

- SWOT analysis of the skills of VTS operators and supervisors

Strengths: - Strong background in maritime navigation - Practical experience in actual ship operations - Experience in the actual functioning of VTS - Strong knowledge of maritime contexts - Strong knowledge of the functioning of the equipment and technologies - Fast processing of the information in different contexts	**Weaknesses:** - Usage of the message markers - Language proficiency and communication
Opportunities: - Improve the use of message markers by implementing exercises in simulated environments - Improve the efficiency of communication internally and externally - Creating more interactive exercises which include VTS environment and ship simulators - Provide training for executing appropriate risk analysis	**Threats:** - Experience influences the involvement of the VTS operators when using the message markers (assuming how the operator would act in the same context) - Internally VTS operators speak local language. The communication with vessels is English. This sometimes causes problems in the fluency of the communication when internal and external communication are combined. - The mandatory reporting of extraordinary events is demanded in VTS centres. Reporting after a finalized work schedule may compromise the quality of the reports.

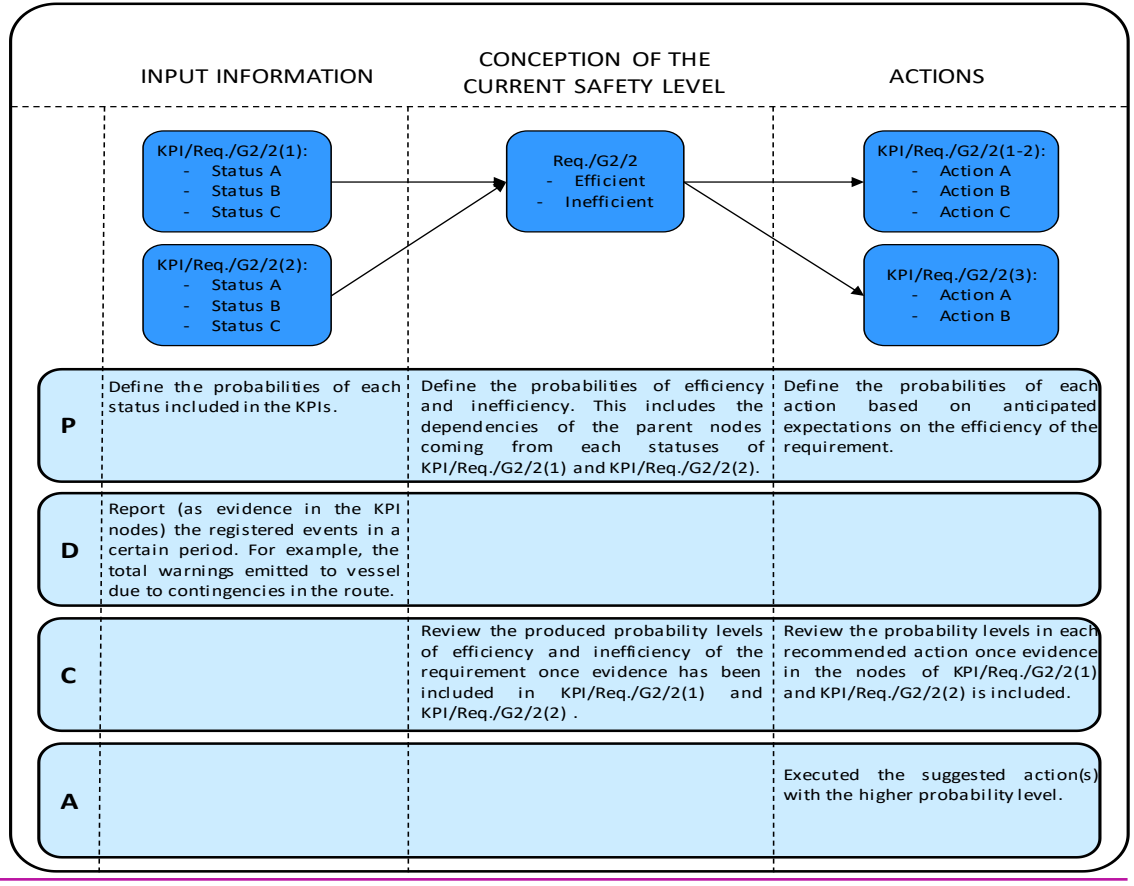
Output (Level 6)

- 31 KPIs for monitoring, measuring and guiding the performance of the designed SMS for VTS Finland

KPIs per requirement
1. KPI/Req./G1/1(1): Percentage of vessel reporting when entering a VTS area (if possible classified by VTS areas) (Monitor KPI) 2. KPI/Req./G1/1(2): Actions developed to improve the vessel reporting (in each VTS area) (Drive KPI) 3. KPI/Req./G1/1(3): The initial status of vessels when entering VTS areas is commonly (Outcome KPI)
4. KPI/Req./G1/2(1): Percentage of efficiency of the VTS monitoring system to represent (portray) ship routes? (Monitor KPI) 5. KPI/Req./G1/2(2): Reported malfunctions compromising AIS? (Outcome KPI)
6. KPI/Req./G1/3(1): Efficiency of the actions made by VTS to ensure vessels listen to the VHF channels? (Monitor KPI) 7. KPI/Req./G1/3(2): Actions developed to improve the information sharing in VTS (Drive KPI)
8. KPI/Req./G2/1(1): Reported speed violations occurred in VTS areas (Monitor KPI) 9. KPI/Req./G2/1(2): Actions made by VTS to efficiently inform about existing restricted areas? (Drive KPI)
10……..

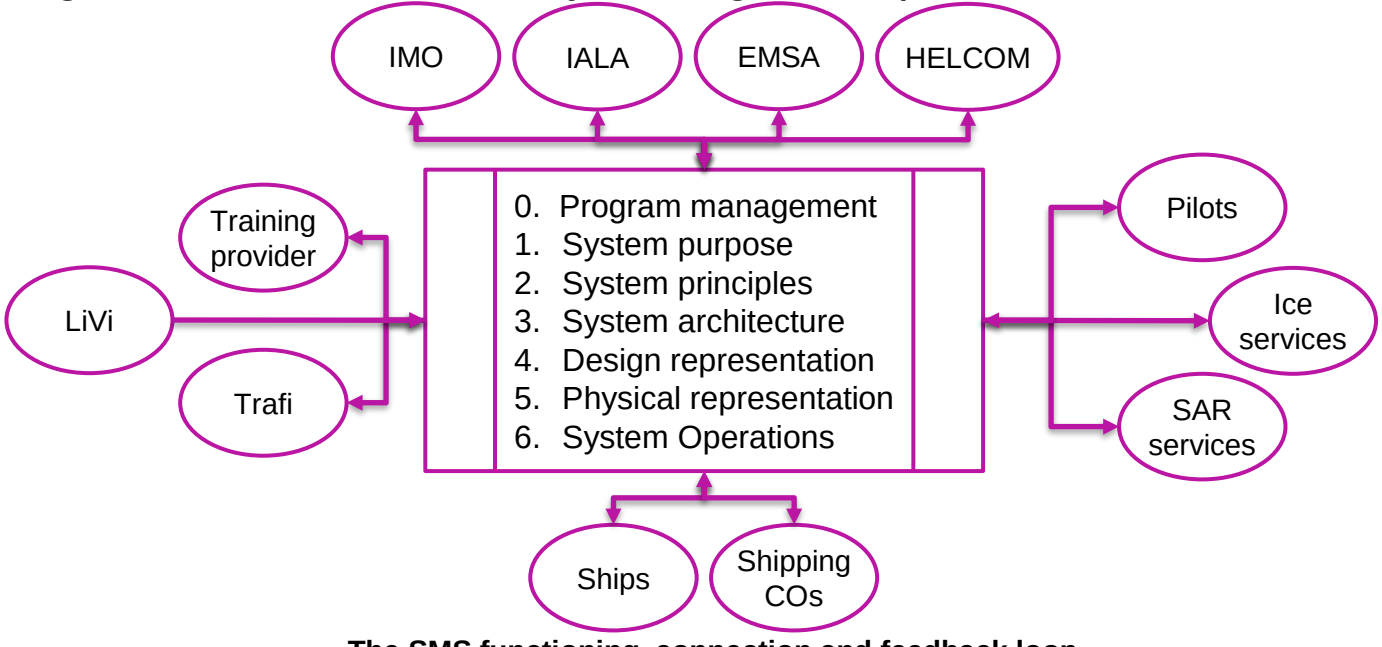
Output (Level 6)

VTS Finland
performance
monitoring tool



Conclusions (1)

The proposed process is capable to adopt the actual safety practices of the organization and transferring these into the functioning of an organizational SMS. This enables a good flow of information with all system stakeholders, improving cooperation and enabling harmonization of safety management practices.



The SMS functioning, connection and feedback loop

Conclusions (2)

- The application of the process resulted in the design of 13 safety requirements utilized to manage the safety of ship traffic in Finnish sea areas all year around.

- Tools have been provided to review the safety performance of the SMS and to revise the objectives and general functioning of the SMS.

- The designed SMS can be utilized and maintained in a smoothly and systemically manner. This prevents making unpredicted and expensive modifications and adaptations afterwards.

- Process downsides: time and resources consuming. Particularly, for an industry heavily educated to operate fast regarding safety and where other approaches (e.g. PRA) are promoted in official guidelines.

Aalto University
School of Engineering

System-Theoretic Process Analysis (STPA)

Aalto University
School of Engineering

STPA process

0. System description and preliminary risk analysis
1. Establish the system engineering foundation for the analysis and for the system development (defining a functional control structure)
2. Identify potentially unsafe control actions
3. Redefine the safety controls
4. Determine how each potentially hazardous control action could occur.

STPA becomes an iterative process with details added as the system design evolves

Issues in the use of STPA

If STPA is an iterative, refinement process, how do I know when I can stop or do I have to go on forever?

In the top-down STPA analysis approach, the analyst can stop refining causes at the point where an effective mitigation can be identified and not go down any further in detail.

How to develop the safety control structure?*

Case Study in Autonomous Shipping

Aalto University
School of Engineering

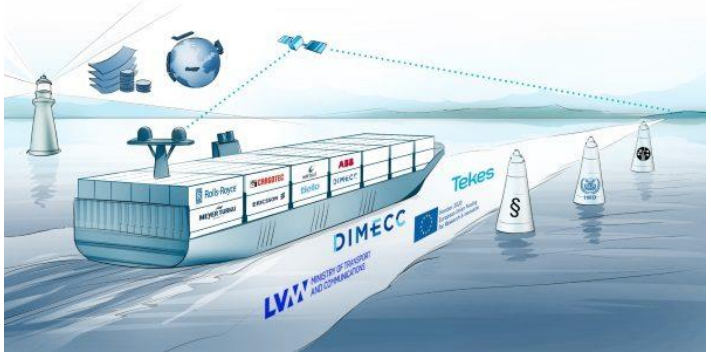
Content

- Definition of **systemic and systematic** risk analysis and management
- **The need** for systemic and systematic risk analysis and management in the context of autonomous vessels
- **Case study:** systemic and systematic risk analysis and management for designing autonomous ferries
- **Summary** (Conclusions)

Systemic Risk Analysis and Management

Systemic

Systemic refers to implementing an efficient approach to cover the different elements of a system(s) that need to be included in the analysis and management of risk [1].

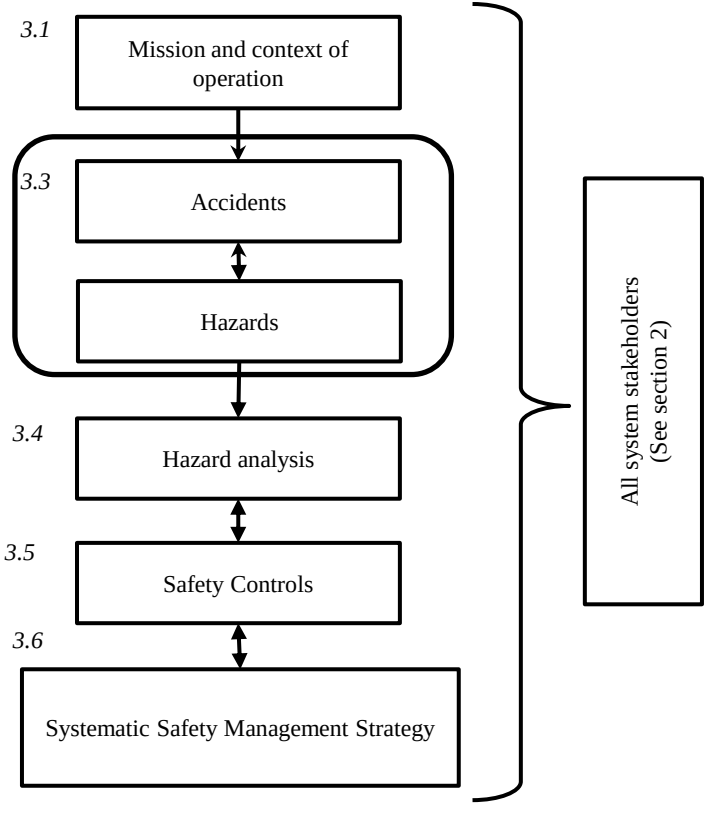


www.oneseaecosystem.net [accessed 02.05.2018]

Systemic Risk Analysis and Management

Systematic

Systematic refers to the need for a methodological approach to analyze and manage the risks of the system(s) under analysis [2].



Why we need a systemic and systematic approach

Why the need for the systemic and systematic approach

What do we know about the safety performance of autonomous vessels?

Recent studies have analyzed and estimated the possible effect on the prevention and response to common maritime accidents such as collisions, groundings, fire on-board, structural failure [3; 4].

However, many of these have been mainly done to hypothetical cases and scenarios.

www.oneseaecosystem.net [accessed 02.05.2018]

Why the need for the systemic and systematic approach

- Autonomous vessel demand understanding of the functioning of the entire systems. This requires the incorporation of **multiple safety viewpoints and interpretations**.

- This approach has to be suitable for increasing the competitiveness of the **maritime transport stakeholders**. It has to provide input information for the elaboration of management models which can consider safety as part of their competitive advantage.

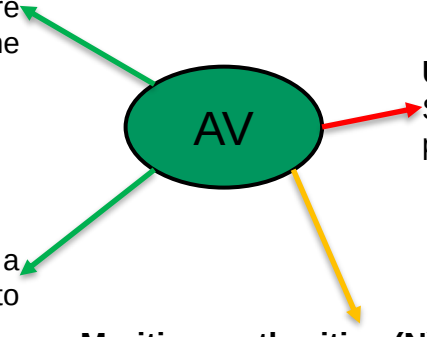
Maritime Transport Stakeholders

Stakeholders

- Marine equipment manufacturers
- Ship owners
- Ship and technology designers
- Ship repairs and offshore yards
- Port and port operators
- Financers and insurances
- Maritime Authorities
- Pilots
- VTS
- SAR services
- Classification societies
- Marine trainers
- Unions
- General public
- ETC.

Stakeholders position towards autonomous vessels and maritime systems

Marine Equipment manufacturers (+)
Marine equipment manufacturers have a positive view towards developing more advanced equipment for ensuring the safety



Unions (-)
Some maritime unions have a stronger posture against autonomous vessels

Ship and technology designers (+)
Designers represent another group with a positive view due to the opportunity to apply innovative designs in shipbuilding

Maritime authorities (N)
Maritime authorities have a neutral perspective and expectative of safety for autonomous vessels

Regulatory challenges related to autonomous ships

Current maritime conventions do not consider autonomous ships

- The most significant challenges concern obligatory crew/shipmaster functions
  - *COLREGs, Rule 5: A ship must always maintain a proper lookout by sight and hearing…*
  - *COLREGS, Rule 2: Requires good seamanship*
  - *STCW: Officers in charge…shall be physically present on the navigation bridge…*
  - *SOLAS, Reg. 24: …autopilot must enable an immediate switch from automatic to manual control*
  - *SOLAS, Reg. 33: The master of a ship is required to assist persons in distress at sea*
- SOLAS allows equivalent solutions, STCW does not
  - *Unmanned operations need to start on internal waters with special permission*
  - *A new international regulatory framework for unmanned ships is needed*

Case Study Description

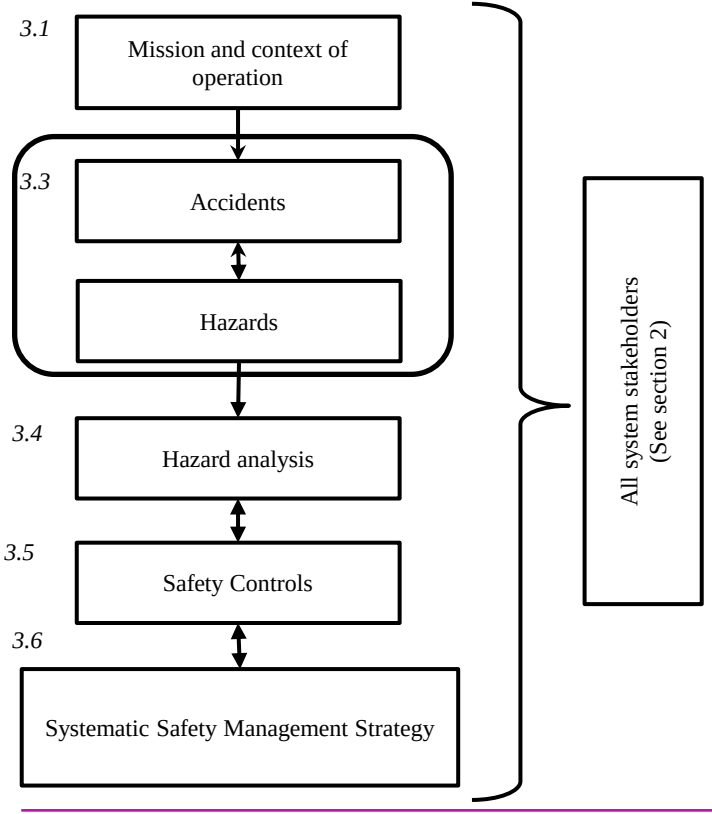
Case Study

This study presents and applies a proposed framework for the analysis of the initial concept design phase of two autonomous ferries [5;6:7].

- The aim is to create a process capable of executing an analysis of safety risks at the **earliest design phase** of the autonomous ferries.
- The analysis produces information to make the systematic and systemic integration of safety controls that need to be included in the initial **safety management strategy** of the vessels.

Valdez Banda, O. A., Kannos, S., Goerlandt, F., van Gelder, P. H., Bergström, M., & Kujala, P. (2019). A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. *Reliability Engineering & System Safety*, *191*, 106584.

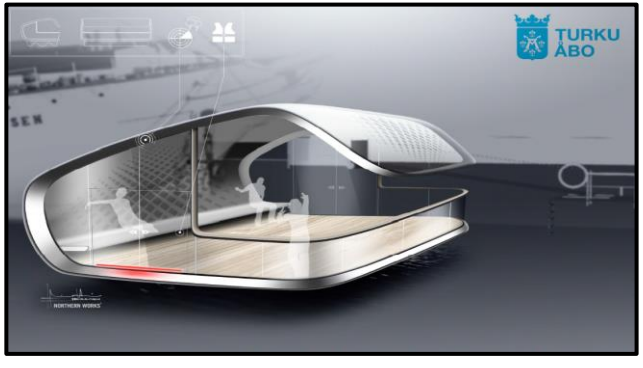
The process



Step	Task
1	Definition of accidents and identification of hazards
2	Detailed hazard description and definition of mitigation actions
3	Definition of the safety controls
4	Unsafe control actions (UCAs) and redefinition of safety controls
5	Representation of the initial safety management strategy

Background

This process is applied to analyze the safety risks in the foreseen functioning of two concepts of autonomous ferries aiming operations in urban waterways in Turku.



- The first concept (ferry A) has a mission to transport passengers from one side to the Aura River in the city of Turku to the other side.
- The second concept (ferry B) has the mission to transport passengers from a location in Turku downtown by the Aura river to a new pier to be located in the Ruissalo Island.

Data

The process uses information produced in:

- Previous maritime risk analysis and,
- **The analysis of the new operational context of these autonomous vessels (expert consultation):**

Lloyd's Register, Suomenlinnan Liikenne Oy, VG-Shipping Oy, Fleetrange Oy, Trafi, ABB, Varsinais-Suomen Pelastuslaitos, Rajavartiolaitos, Uudenkaupungin Työvene Oy, Besase Oy, Arctia Shipping Oy, Yrkeshögskolan Novia, Aalto Yliopisto, Metropolia Ammattikorkeakoulu, SSF Oy, Paikkatietokeskus FGI, Rosita Oy, Meriturva, Turun kaupunki.

Process: step one

Definition of accidents and identification of hazards

- 10 accidents covered
- 15 Hazards identified and analyzed
- Clear interconnection among accidents and hazards
- Combinatorial analysis of current accidents and expected accidents for autonomous vessels

Accident	Hazards
1. Allision with a pier	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical failure) H4. Heavy weather/sea conditions H5. Strong currents H6. Position reference equipment failure
2. Collision with a moving object	
2.1 Collision with another vessel	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical fault)
2.2 Collision with a small moving target (e.g. canoe, SUP-board, etc.)	H1. Object detection sensor error H2. AI software failure H3. Technical failure (e.g. mechanical failure)
3. Collision with a fixed object (e.g. buoys, beacons, etc.)	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical failure) H4. Heavy weather/sea conditions H5. Strong currents H6. Position reference equipment failure
4. Grounding	H2. AI software failure H3. Technical failure (e.g. mechanical failure) H6. Position reference equipment failure H4. Heavy weather/sea conditions H5. Strong currents
5. Bottom touch	H2. AI software failure H3. Technical failure (e.g. mechanical failure) H6. Position reference equipment failure H4. Heavy weather/sea conditions H5. Strong currents
6. Capsizing/ Sinking	H7. Overloading of the vessel H8. Shifting of weights H9. Flooding
7. Fire on board	H10. Ignition of electrical equipment or wiring H11. Passenger starting a fire
8. Man over board	H12. Unintended falling overboard H13. Intended jumping overboard
9. Medical emergency on board	H14. Person(s) getting injured H15. Person(s) medical condition
10. Medical emergency on pier	H14. Person(s) getting injured H15. Person(s) medical condition

Process: step two

Detailed hazard description and definition of mitigation actions

Hazard	H1. Object detection sensor error		
Hazard effect/ description	What exactly? How severe?		
Causal factors	Potential causes?		
Mitigation actions	What can we do? How to mitigate/control it?	Cost/Difficulty High Low Medium Medium Low Low Low	Approach (1-4) * 4 3 3 4/3 3 3 2

*Mitigation approach	Level	Detailed description
	4	Attempt to completely eliminate the hazard
	3	Attempt to reduce the likelihood that the hazard will occur
	2	Attempt to reduce the likelihood that the hazard results in an accident
	1	Attempt to reduce the damage if the accident occurs

Process: step three

Defining safety controls based on the adopted mitigation actions

This step demands the review and prioritization of the mitigations actions that will be further developed as the safety controls of the initial safety management strategy.

The aim is to assess (together with experts) if the safety controls are objective and relevant to continue their analysis.

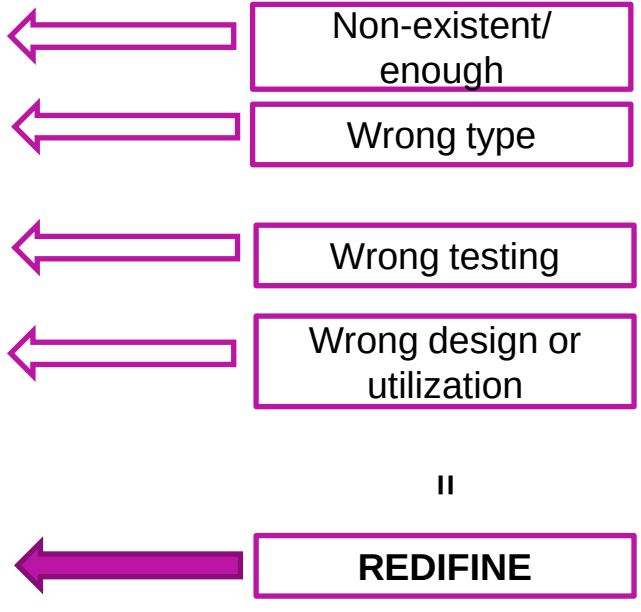
Mitigation approach*	Code	Safety controls
H1. Object detection sensor error		
4	SC 1	Sensor system redundancy and diversity
3	SC 1	UPS (Uninterrupted Power Source)
	SC 2	Appropriate heating, cooling, and cleaning systems
	SC 3	Thorough commissioning of equipment set
	SC 4	Appropriate and continuous on board maintenance program
	SC 5	Continuing system diagnosis and proof testing
2	SC 1	Autonomous Integrity monitoring

*Mitigation approach	Level	Detailed description
	4	Attempt to completely eliminate the hazard
	3	Attempt to reduce the likelihood that the hazard will occur
	2	Attempt to reduce the likelihood that the hazard results in an accident
	1	Attempt to reduce the damage if the accident occurs

Process: step four

Unsafe control actions (UCAs) and redefinition of safety controls: how the safety control can fail and why?

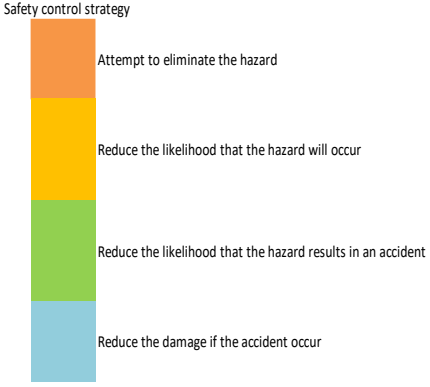
Safety controls (mitigation approach)
SC 1 Sensor system redundancy and diversity
Detecting potentially Unsafe Controlled Actions (UCAs) and redefining the safety control
UCA 1. Sensor does not function properly and there is no other sensor available
Potential causes
- Lack of economic resources
UCA 2. Equipment chosen to provide the redundancy are not suitable
Potential causes
- Lack of economic resources
- Lack of knowledge of sensors characteristics when planning the equipment set needed
UCA 3. Sensor failure is not detected
Potential causes
- Not enough coverage with the diagnosis
UCA 4. External or common cause failures takes several equipment down at the same time
Potential causes
- Inappropriate system design
- Incorrect installation
- Incorrect usage
- Environmental conditions
Redefining of the safety control
- If one sensor fails the redundancy ensures there is going to be another sensor functioning
- Equipment chosen to provide the redundancy have to be the correct ones in order to provide the user with the required information at all times



Process: step five

Representation of the initial safety management strategy

Hazard	Safety Control (SC)	Control logic principle	Risks mitigated
1	1. Object detection sensor error		
1. Object detection sensor error	1. Sensor system redundancy and diversity	If one sensor fails the redundancy ensures there is going to be another sensor functioning. The quipment chosen to provide the redundancy has to be the correct in order to provide the user with the required information at all times	> Innapropriate functioning and availability of the sensor > Correctness on the selection of redundancy equipment on time detection sensor failure > External failures affecting the functioning of the sensor
	1. UPS (Uninterrupted Power Source)	If there is a disturbance in the vessel power system the UPS can temporarily provide power for the critical equipment. When the UPS setup is planned, installed and maintained properly, the user can count on a reliable backup system	> There is a disturbance in vessel's power system and the equipment is not backed up with UPS > The UPS does not work or take too long to switch on > The capacity of the UPS is not sufficient to provide power for the equipment
	2. Appropriate heating, cooling and cleaning systems	By applying sensors with proper heating and/or cooling systems it can be ensured that they function properly in all operating conditions. Proper automatic cleaning systems can ensure the appropriate function of the sensors outdoors	> Equipment is not able to function properly in winter conditions > Equipment is not able to function properly due to the high temperature > Equipment lens is dirty > Condensation inside equipment
	3. Thorough commissioning of equipment set	When the equipment set is thoroughly tested and certified (preferably by an independent body) it ensures that the equipment functions properly, is compatible and the operation can be run safely.	> The equipment set has not been properly tested or not tested at all before operation
	4. Appropriate and continuous on board maintenance programs	By implementing a maintenance program it can be ensured that all critical systems remain functional at all times. A well planned maintenance program covers all necessary areas on board and it is adjusted separately for each vessel. Maintenance done timely and accordingly to the program by competent personnel ensures the smooth operation of the sensors.	> There is no maintenance program > The maintenance program does not cover the necessary elements and the life cycle of the hardware > The maintenance program is not followed or it is wrongly applied
	5. Continuing system diagnosis and proof testing	Continuing system diagnosis and regular proof testing ensures that the system functions as it should. Test design should be planned carefully and updated after changes in the system in order to cover all the necessary functions and recognize potential problems. Possible effect on the operation should be taken into account in planning	> There is not continuing system diagnosis and proof testing > The continuing system diagnosis and proof testing does not cover all necessary functions > The test is not able to recognize problems
	1. Autonomous integrity monitoring	Well designed and up to date integrity monitoring system ensures that the data has not been damaged or manipulated	> There is not integrity monitoring > Integrity monitoring gives wrong information



Process: step five

Representation of the initial safety management strategy

Safety Control (SC)	Accident 1	2,1	2,2	3	4	5	6	7	8	9	10
1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1	H1		H10			
2	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H10			
3	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H11			
4	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
5	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
6	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H8		H12		
7	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H9		H12		
8	H4 H2	H2	H2	H4 H2	H4 H2	H4 H2	H7 H9		H12		
9	H3	H3	H3	H3	H3	H3	H7	H11	H12		
10	H3	H3	H3	H3	H3	H3	H7	H11		H14	H14
11	H4			H4	H4	H4	H7	H11		H14	H14
12	H4			H4	H4	H4	H8			H14	H14
13	H6			H6	H6	H6	H8			H14	H14
14	H6			H6	H6	H6	H9				
15	H6			H6	H6	H6	H9				
16	H6			H6	H6	H6	H8	H10			
17							H8		H12		
18							H9		H12		
19							H9			H14	H14
20								H10			
21								H10			
22								H10			
23								H11			
24								H11			
25									H12	H12	H12
26									H12		
27										H14	H14
Total SC	31	16	16	31	25	25	15	12	10	9	9

SC control strategy:

- Attempt to eliminate the hazard
- Reduce the likelihood that the hazard will occur
- Reduce the likelihood that the hazard results in an accident
- Reduce the damage if the accident occur

Study Case Conclusions

The process produces itemized information **to guide (with information of safety demands) the initial design** of the autonomous ferry and its operational system.

The logic principle of the safety controls provides the **foundations for developing a safety management strategy** at the earliest design phase.

The study results support the elaboration of **plans, conceptual designs, ship arrangements, and the setting** of other crucial elements for designing and building the autonomous ferry.

Summary (Conclusions)

Systemic and systematic risk analysis and management aims at defining, measuring and handling the dangers to individuals, organizations, property and businesses in certain system(s) and with a defined method.

The analysis and management of the risk and safety in autonomous vessels and maritime systems demands the consideration of **multiple safety viewpoints and interpretations**.

Systemic and systematic risk analysis processes are needed to produce itemized information to **guide the initial design of an autonomous vessels** and its operational system.

More details about the case study

Valdez Banda, O. A., Kannos, S., Goerlandt, F., van Gelder, P. H., Bergström, M., & Kujala, P. (2019). A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. *Reliability Engineering & System Safety*, *191*, 106584.

Conclusions on STPA

- STPA is a powerful tool to develop hazard analysis
- It provides qualitative information for risk analysis and to determine potential actions for preventing, controlling or mitigating system hazards
- It is flexible to adapt it to the needs or demands of the safety system.
- Provokes having a system ready to face hazards. So, it does not focus on making components reliable only.
- Downsides: time and resources consuming. Unclear when to stop.

Course assignment

Relevant for the STPA application

Learning logs

Please return the third learning log by Sunday 3.10 at 23:59

Time for the fast quiz

Instructions:

- The fast quiz is open after the finalization of Lecture 3 (so, now)
- The link to the quiz is:

- The link will close at 14:00
- The grading of the quiz is given before Lecture 04
- We keep online via zoom during the time of the quiz. So, if you have any question, please let me know

Aalto University
School of Engineering

MEC-E2009 - Marine Risks and Safety L

Thank you

Osiris A. Valdez Banda