Aalto University
School of Engineering

Automaattisen merenkulun turvallisuus merellä

Osiris A. Valdez Banda, Pentti Kujala

Aalto University

INTELLIGENT SHIPPING TECHNOLOGY

Älykkään merenkulun työ- ja kutsuseminaari 23.–24.8.2018, Rauma

The need for a systemic and systematic risk analysis and management

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 and systematic risk analysis and management

Aalto University
School of Engineering

Systemic Risk Analysis and Management

Systemic

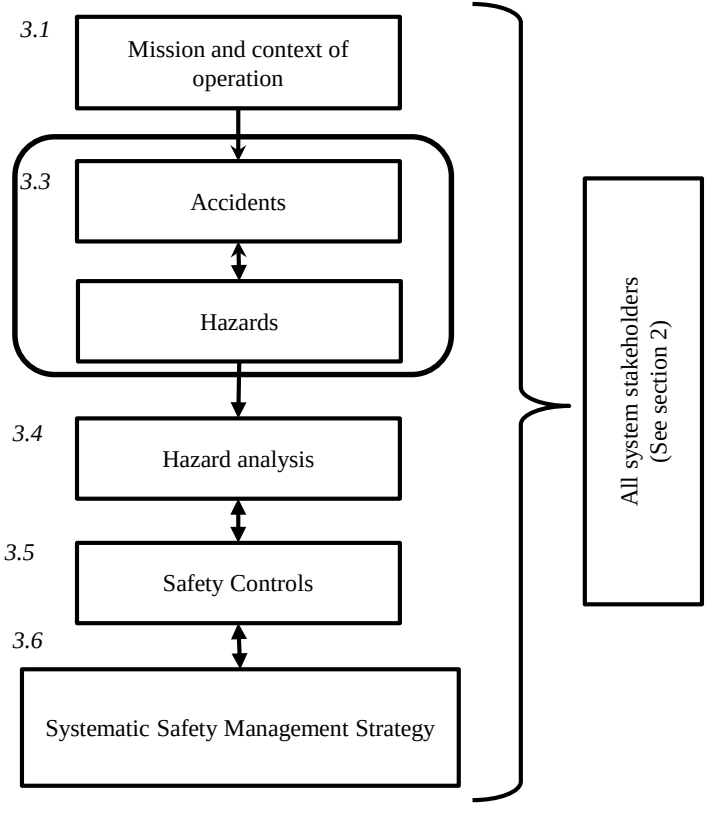
Systemic refers to implementing an efficient approach to cover the different elements of a system(s) that need to be included in the analysis and management of risk [1].

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.

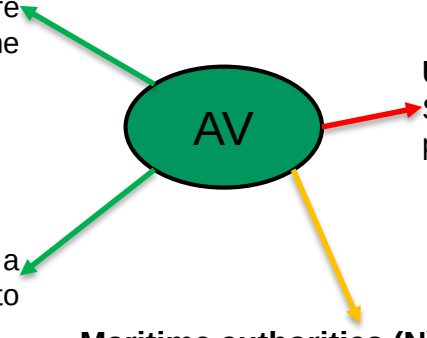
Maritime Transport Stakeholders

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*

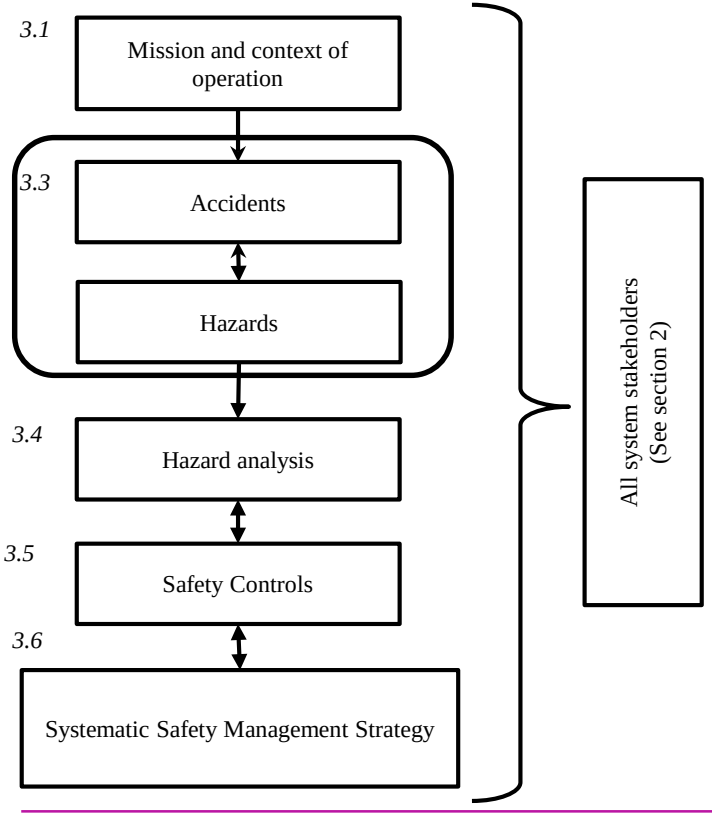
Case study

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.

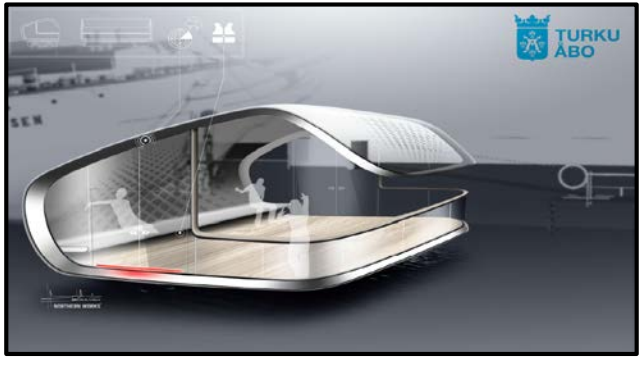
The process



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.

Methodology foundations

The proposed process is based on a **System- Theoretic Process Analysis (STPA)** included within the **Systems-Theoretic Accident Modelling and Processes (STAMP)** [8].

- STAMP is a relative new approach to depict and review the function of safety from a systemic perspective.
- STPA is a hazard analysis technique that identifies accident scenarios that encompass the entire accident process.

The aim of the proposed process is to **support** the subsequent design stages with the provision of valuable information to ensure safety.

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.

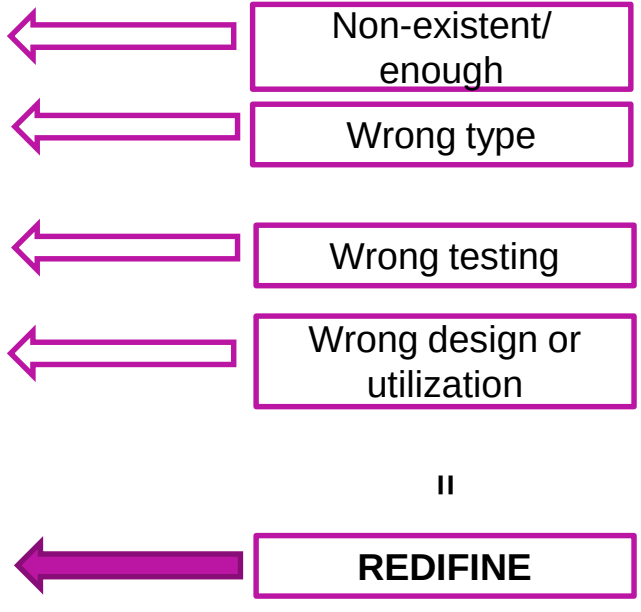
Mitigation approach*	Code	Safety controls
H1. Object detection sensor error		
4	SC 1	Sensor system redundancy and diversity
3	SC 1	UPS (Uninterrupted Power Source)
	SC 2	Appropriate heating, cooling, and cleaning systems
	SC 3	Thorough commissioning of equipment set
	SC 4	Appropriate and continuous on 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?

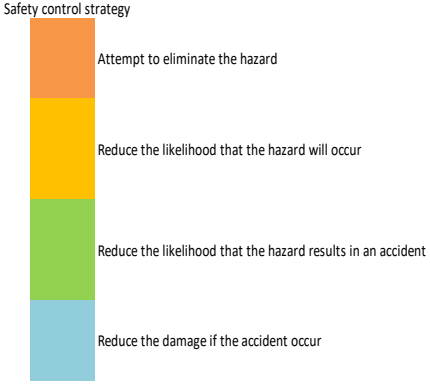
Safety controls (mitigation approach)
SC 1 Sensor system redundancy and diversity
Detecting potentially Unsafe Controlled Actions (UCAs) and redefining the safety control
UCA 1. Sensor does not function properly and there is no other sensor available
Potential causes
- Lack of economic resources
UCA 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.

More details about the case study

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, including changes in the regulatory framework**.

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.

Questions

Research carried on:

References

1. Kaplan, S., 1997. The Words of Risk Analysis. Risk Analysis, An International Journal. Society for Risk Analysis.
2. Valdez Banda, O.A. Kujala, P., Goerlandt, F., Bergström M., Ahola, M., van Gelder P.H.A.J.M., Sonninen S. 2018. The need for systematic and systemic safety management for autonomous vessels. IMDC 2018.
3. Wróbel, K., Krata, P., Montewka, J. and Hinz, T. 2016. "Towards the Development of a Risk Model for Unmanned Vessels Design and Operations." TransNav : International Journal on Marine Navigation and Safety of Sea Transportation Vol. 10 nr 2.
4. Wróbel, K., Montewka J., and Kujala, P. 2017. "Towards the Assessment of Potential Impact of Unmanned Vessels on Maritime Transportation Safety." Reliability Engineering & System Safety 165 (September):155–69
5. Valdez Banda, O.A., Kannos, S., Goerlandt, F., , van Gelder, P.H.A.J.M, Bergström, M., and Kujala, P. A systematic and systemic hazard analysis and management process for the concept design phase of an autonomous vessel within its operative context. Submitted to Reliability Engineering and System Safety.
6. ISSAV International Seminar Autonomous Vessels. Presentations. Found at: https://www.tudelft.nl/en/events/2018/tu-delft/03-march/international-seminar-autonomous-vessels-issav/
7. Smart City Ferries (ÄLYVESI) project. Project webpage: http://www.aboamare.fi/About-ÄlyVESI
8. Leveson, N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.