Application of various methods for safety assessment of autonomous ships

Jakub Montewka
Finnish Geospatial Research Institute
Gdynia Maritime University

Krzysztof Wróbel
Gdynia Maritime University

NIN/NFAS Seminar, NTNU Trondheim
June 15, 2017

Agenda

- **Introduction**
- **Methods suitable for safety assessment and preliminary results**
  - What-if analysis
  - Causal model
  - System-theoretic approach
- **Conclusions**

NLS
FINNISH GEOSPATIAL RESEARCH INSTITUTE
FGI

Introduction

Unmanned vessels:

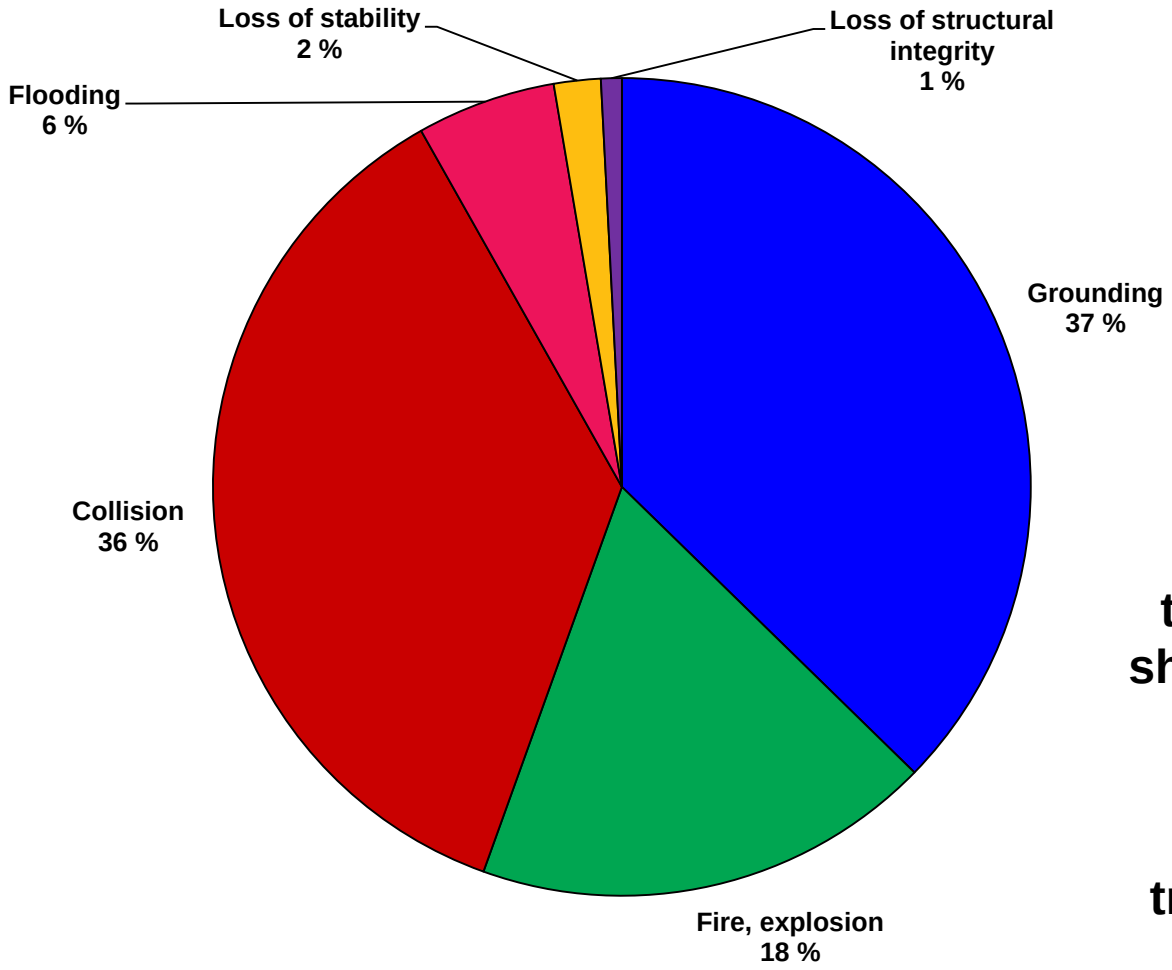
- Expected to enter into operation by the mid of next decade
- No or extremely limited crew on board
- Operating by remote control or autonomously
- Highly-advanced technology
- Environmentally friendly
- Cost-effective
- Safe?

AAWA. (2016). Remote and Autonomous Ships The next steps. London.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Introduction

’Manned’ shipping accidents by type - global values

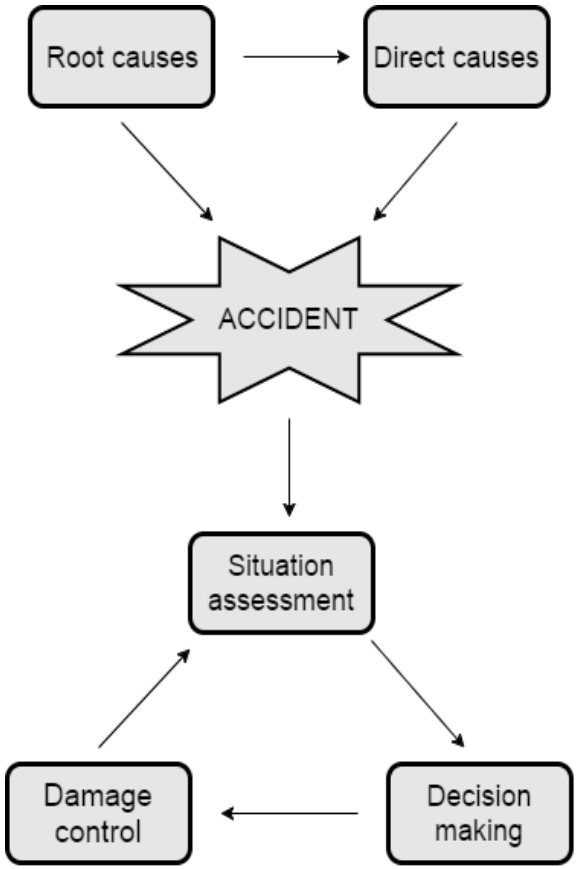


How to ensure that unmanned ships at least do not reduce the safety of maritime transportation?

European Maritime Safety Agency. Annual Overview of Marine Casualties and Incidents 2014. Lisbon: 2015.

NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI

What-if analysis of autonomous vessels safety



WHAT-IF ANALYSIS

EVALUATION OF UNMANNED SHIP'S ACCIDENT'S LIKELIHOOD:

1. Assess qualitatively the potential occurrence of each HFACS-MA causal category in future maritime accidents where unmanned ships are involved;
2. Review historical accident reports for manned ships to determine the causal factor(s) leading to the accidents;
3. Attribute each defined causal factor to causal categories as per HFACS-MA;
4. Assess qualitatively the impact of the unmanned ships' introduction on accident's likelihood, based on knowledge extracted in Step 3 and classification scheme in Step 1.

EVALUATION OF ACCIDENT'S CONSEQUENCES:

1. Determine impact on unmanned ship's accident output based on outcome factors.

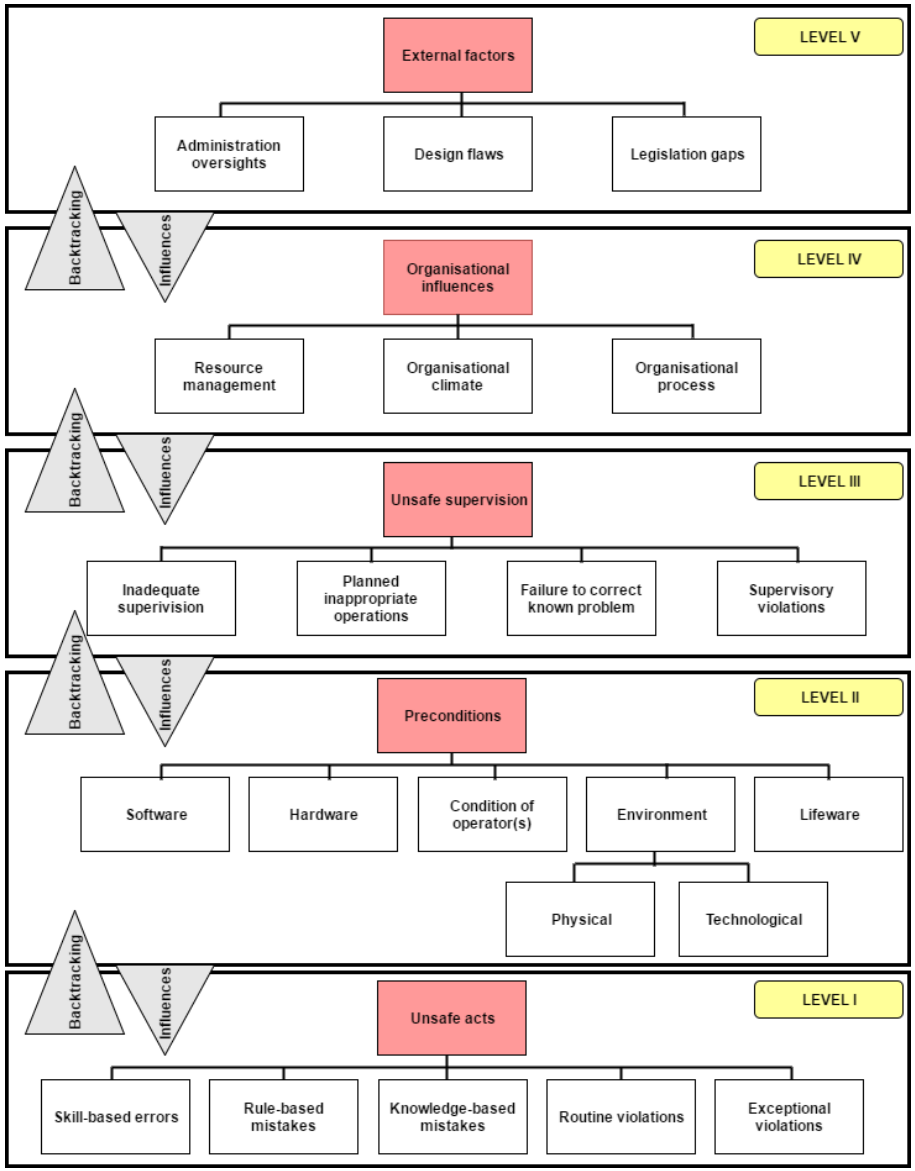
LIKELIHOOD AND CONSEQUENCES ASSESSMENT

K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

What-if analysis – accident likelihood

The overview of HFACS-MA framework applied



K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

What-if analysis – accident likelihood

Brief description of HFACS-MA causal categories applied

Level V: External factors	
Legislation gaps	The deficiencies of existing rules or codes that guide the maritime industry and relevant authorities [34]
Administration oversights	The deficiencies of the governing authorities in implementing the existent rules or codes, or the negligence in performing their duties
Design flaws	Poor system design, such as poor consideration on ergonomics and maintainability of the system/components [35]
Level IV: Organisational influences [36]	
Resource management	Encompasses the realm of corporate-level decision making regarding the allocation and maintenance of organisational assets (such as personnel, money, equipment and facilities)
Organisational climate	The working atmosphere within the organisation which includes culture, policies and structure
Organisational process	Refers to corporate decisions and rules that govern the everyday activities within the organisation. This includes the establishment/use of standard operational procedures and formal methods for maintaining oversight of the workforce
Level III: Unsafe Supervision	
Inadequate supervision	The factors that supervision fails to identify a hazard, recognise and control risk, provide guidance, training and/or oversight etc., resulting in human error or an unsafe situation
Planned inappropriate operation	The factors that supervision fails to adequately assess the hazards associated with an operation and allow for unnecessary risk
Failure to correct known problem	The factors that supervision fails to correct known deficiencies in documents, processes or procedures, or fails to correct inappropriate or unsafe actions of individuals create an unsafe situation
Supervisory violations	The factors that supervision wilfully disregards instructions, guidance, rules or operating instructions whilst managing organisational assets create an unsafe situation
Level II: Preconditions [37]	
Condition of operator(s)	The conditions of an individual that have adverse influence to perform his/her job, i.e. mental and physiological status and mental/physical limitations of the practitioners
Software	The non-physical part of the system including organisational policies, manuals, checklist layouts, charts, maps, advisories and computer programs
Hardware	The physical part of the workplace. It includes the equipment of work stations, displays, controls and seats, etc.
Physical environment	The factors of nature environment which can affect the actions of individuals result in human error or an unsafe situation
Technological environment	The factors emphasise on the artificial environmental constructions, e.g. harbours, waterways and traffic control issues
Liveware	The peripheral livewares refer to the system's human-human interactions including such factors as managements, supervision, crew interactions and communications
Level I: Unsafe acts	
Skill-based errors	Errors involve slips and lapse. Slips are an unintentional action where the failure involves attention whilst lapses are an unintentional action where the failure involves memory [37]
Rule-based mistakes	Mistakes involve inappropriate matching of environmental signs to the situational component of well-tried troubleshooting rules [32]
Knowledge-based mistakes	Mistakes happen when an individual has run out of applicable problem-solving routines and is forced to work 'on-line', using slow, sequential, laborious and resource limited conscious processing [32]
Routine violations	Causal factors tend to be habitual by nature and often tolerated by governing authority [38]. They occur every day as people regularly modify or do not strictly comply with work procedures, often because of poorly designed or defined work practices [37]
Exceptional violations	Causal factors tend to be a one-time breach of a work practice, such as safety regulations being deliberately ignored to carry out a task. Even so, the intention was not to commit a malevolent act but just to get the job done [37]

Indicates accident's likelihood greater for unmanned vessels in the applied framework
Indicates accident's likelihood lesser for unmanned vessels
Indicates neutral impact on the likelihood of the unmanned vessels' accident

K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

What-if analysis – accident consequences

We assigned the value of ‘consequences greater for unmanned ships’ whenever at least one of the following outcome factors was identified in an accident report:

- crew had to directly intervene by either inspecting ship’s enclosed spaces or manually reconfiguring its sub-systems;
- crew had to cooperate with other actors under pressure of time;
- crew was obligated to assist other seafarers should the vessel they collided with need to be abandoned;
- decisions on further actions could not be efficiently taken from remote command post;
- better maintenance of on board equipment before accident could have limited its outcome.

We assigned the value of ‘consequences lesser for unmanned ships’:

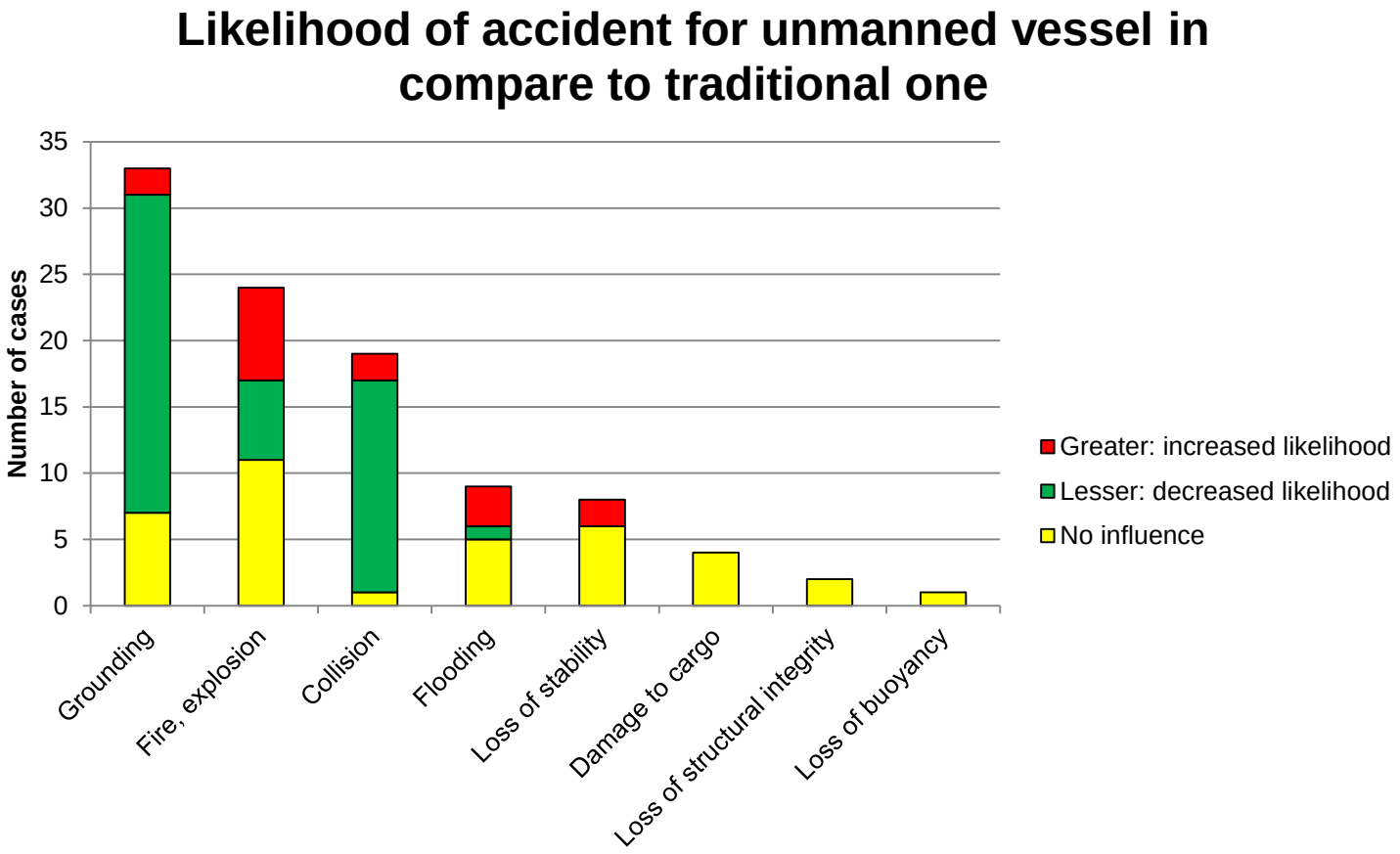
- whenever an accident report mentioned fatalities, serious injury or it was evident that humans’ presence on board during an accident restricted number of possible options of counteracting the effects of accident (e.g. when a person was missing in muster station and so CO_2 could not be released);

Should the circumstances of ‘greater’ and ‘lesser’ outcome occur simultaneously, the value was assigned based on more detailed analysis regarding which of them would be more relevant, with potential for avoiding fatalities greatly lowering the hypothetical consequences.

NLS
FINNISH GEOSPATIAL
RESEARCH INSTITUTE
FGI

What-if analysis - results

How will the autonomous vessels affect maritime safety?

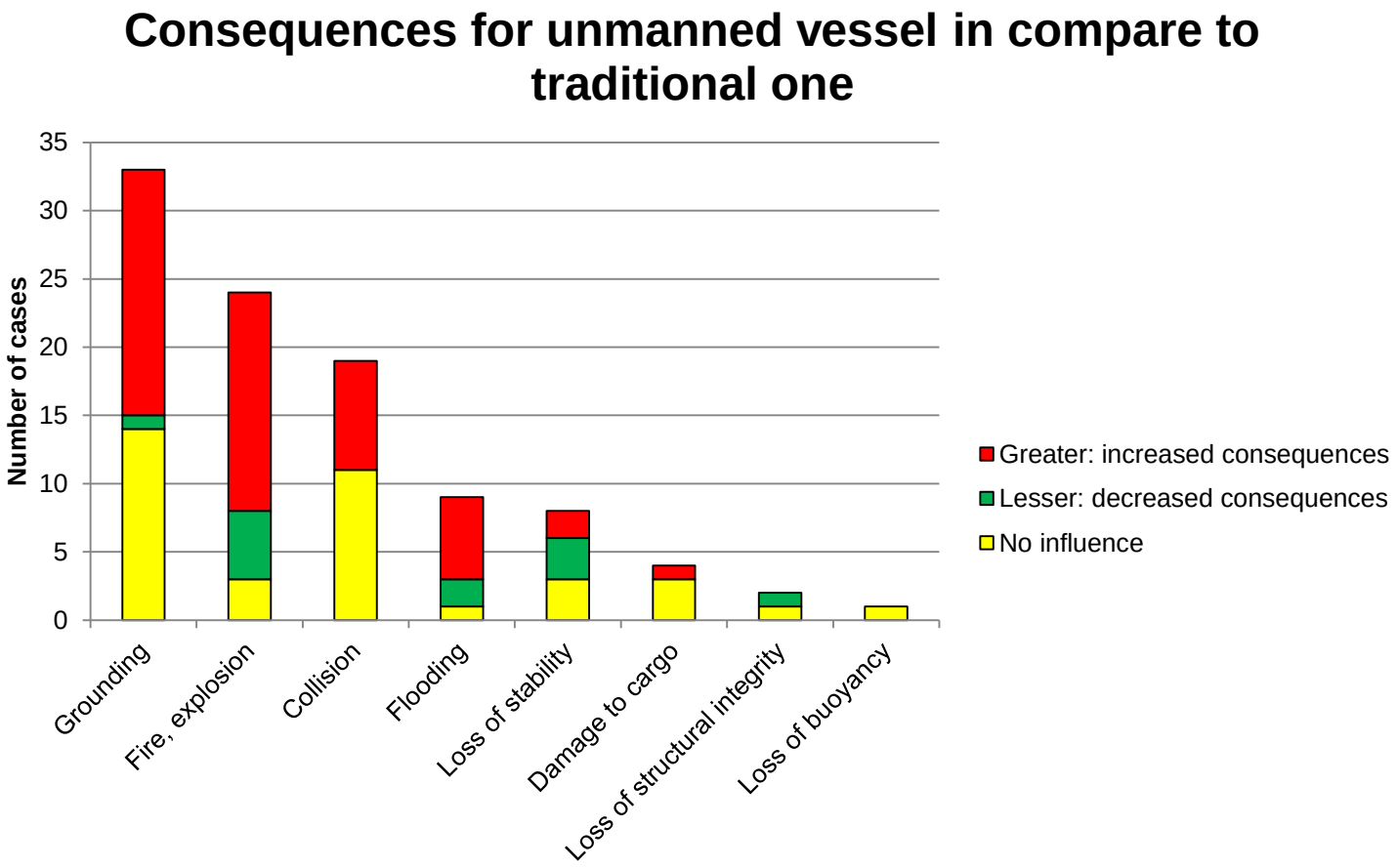


K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

What-if analysis - results

How will the autonomous vessels affect maritime safety?

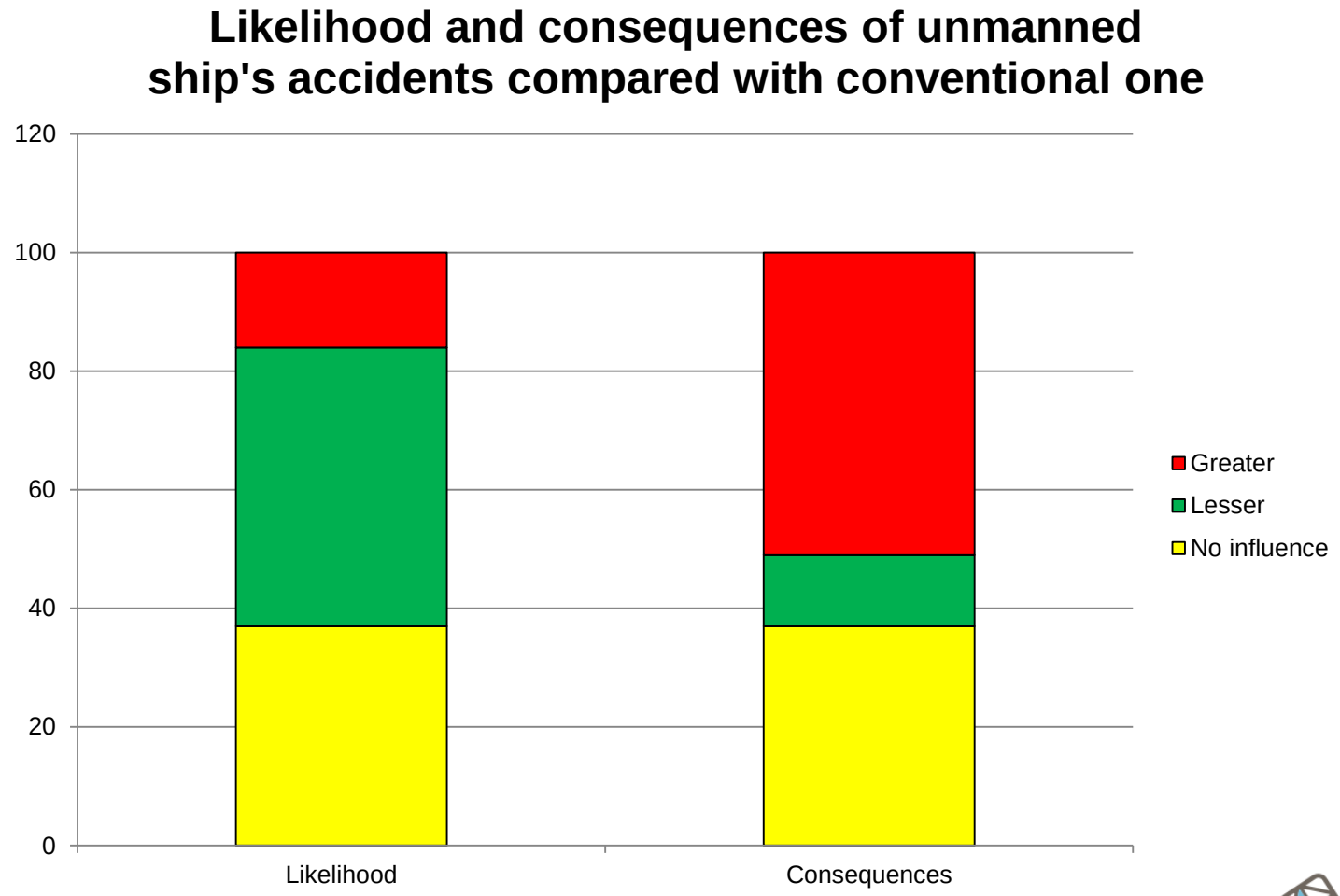


K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

What-if analysis - results

How will the autonomous vessels affect maritime safety?

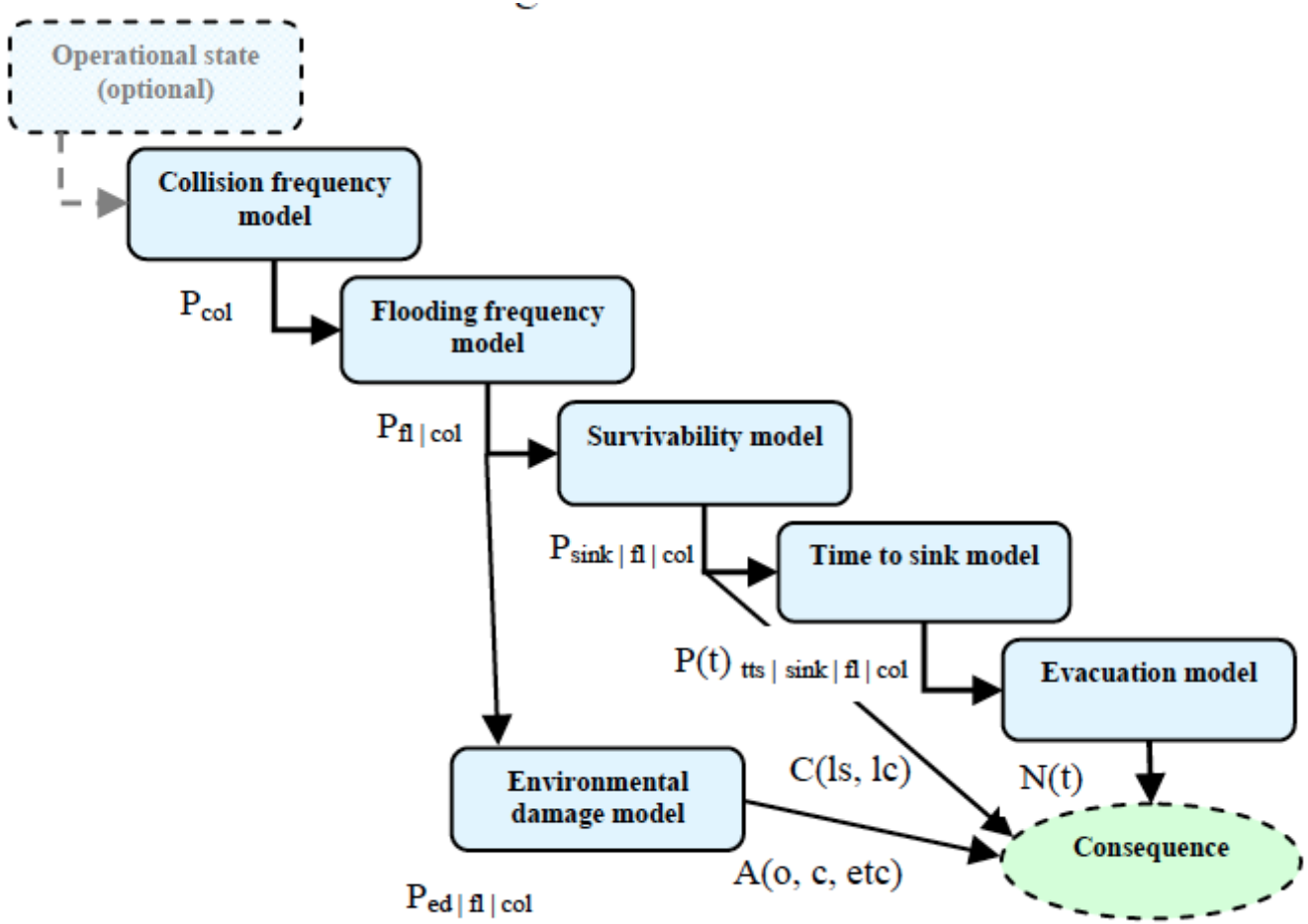


K. Wróbel, J. Montewka, and P. Kujala, "Towards the assessment of potential impact of unmanned vessels on maritime transportation safety," Reliab. Eng. Syst. Saf., vol. 165, no. September, pp. 155–169, 2017.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Causal model

A standarized risk model for ship-ship collision



E. Vanem, R. Puisa, and R. Skjong, "Standardized Risk Models for Formal Safety Assessment of Maritime Transportation," in Proceedings of the ASME 28th International Conference on Ocean, Offshore and Arctic Engineering OMAE, 2009, pp. 51–61.

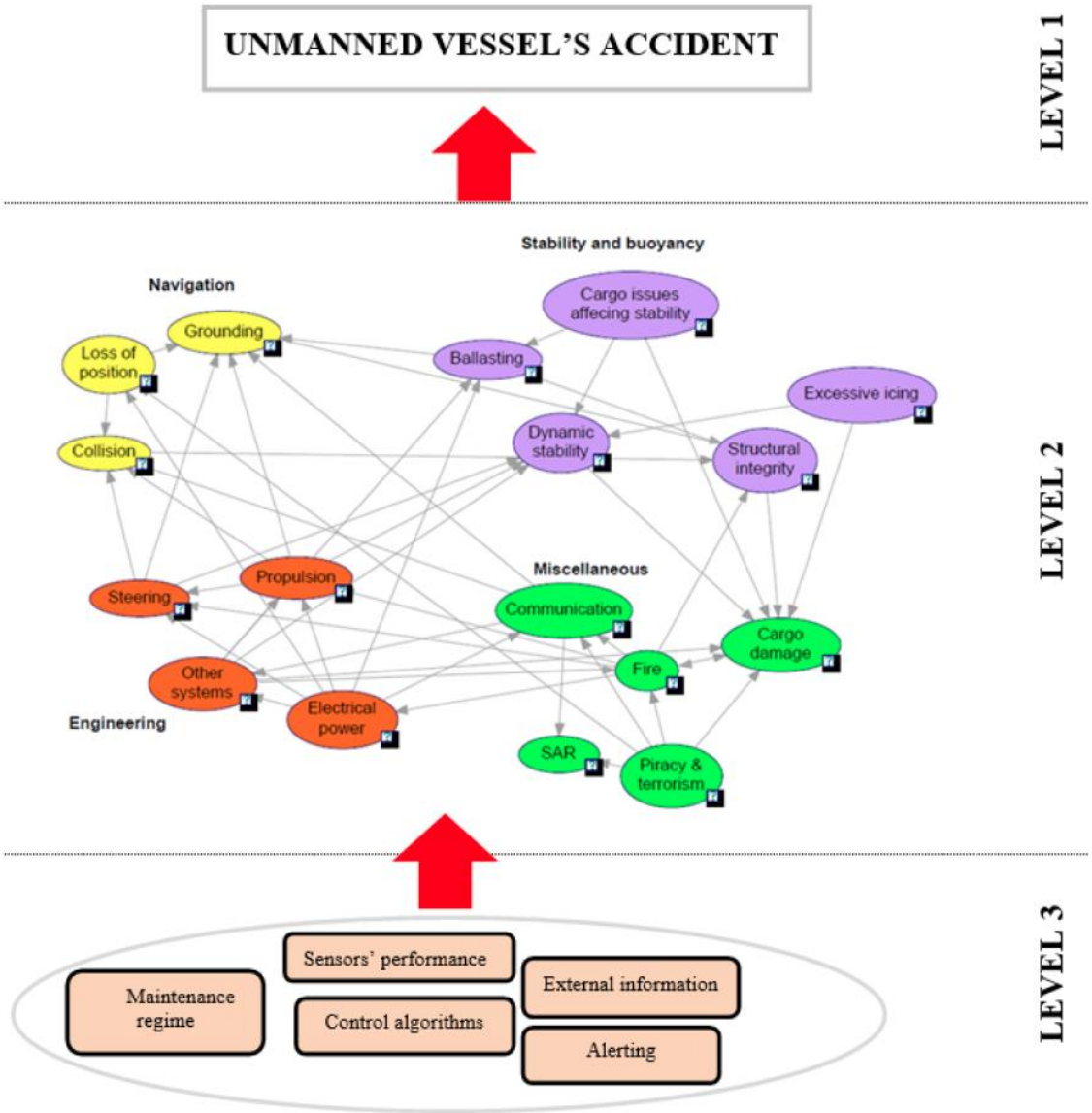
NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Causal model

Tentative list of hazards for autonomous ships

#	Description of hazard
1	Vessel's physical interaction with manned structures results in death or injury
1.1	Vessel collides with another ship
1.2	Vessel runs into an element of infrastructure (i.e. bridge)
1.3	Vessel damages other man-made objects (i.e. fishing gear)
1.4	Vessel is incapable of properly containing dangerous chemicals or energy
1.5	Vessel causes death or injury to persons accidentally or illegally occupying her compartments
1.6	System does not detect a distress situation
2	Vessel's inability to reach port of destination in expected time
2.1	Vessel runs aground
2.2	Vessel suffers from propulsion/steering failure
2.3	Vessel is denied passage due to security concerns
2.4	Vessel's her navigational capabilities are impaired by weather conditions
2.5	Vessel suffers from loss of stability
2.6	Vessel suffers from flooding
3	Vessel's inability to deliver cargo in unchanged condition or in a condition that falls within industry standard
3.1	Vessel loses her cargo at sea
3.2	Vessel is unable to maintain proper cargo stowage conditions
4	Vessel's exposure to major damage or breakdown
4.3	Vessel suffers from fire or explosion
4.4	Vessel suffers from loss of structural integrity
4.5	Vessel suffers from loss of power supply
4.6	Contact with the vessel cannot be established
5	Vessel's inability to prevent environmental pollution
5.1	Vessel is unable to maintain integrity of tanks containing oils or oily mixtures
5.2	Vessel is unable to maintain proper fuel combustion parameters
6	Vessel's interaction with third-party assets causes reduction of their value or operational abilities
6.2	Vessel contributes to delay of other ships' traffic
6.3	Vessel violates international or coastal state's regulations
6.4	System's communication subsystem unintentionally interferes with other assets
6.5	System causes other vessel to ground, run into element of infrastructure or damage other man-made objects

Causal model



- Model of potential failure propagation during the autonomous vessel's accident
- Model allows for safety quantification in terms of risk level
- Major challenge – lack of data
- Other (qualitative) methods may be better to elaborate on safety and the ways to control it

K. Wrobel, P. Krata, J. Montewka, and T. Hinz, "Towards the Development of a Risk Model for Unmanned Vessels Design and Operations," TransNav, Int. J. Mar. Navig. Saf. Sea Transp., vol. 10, no. 2, pp. 267–274, 2016.

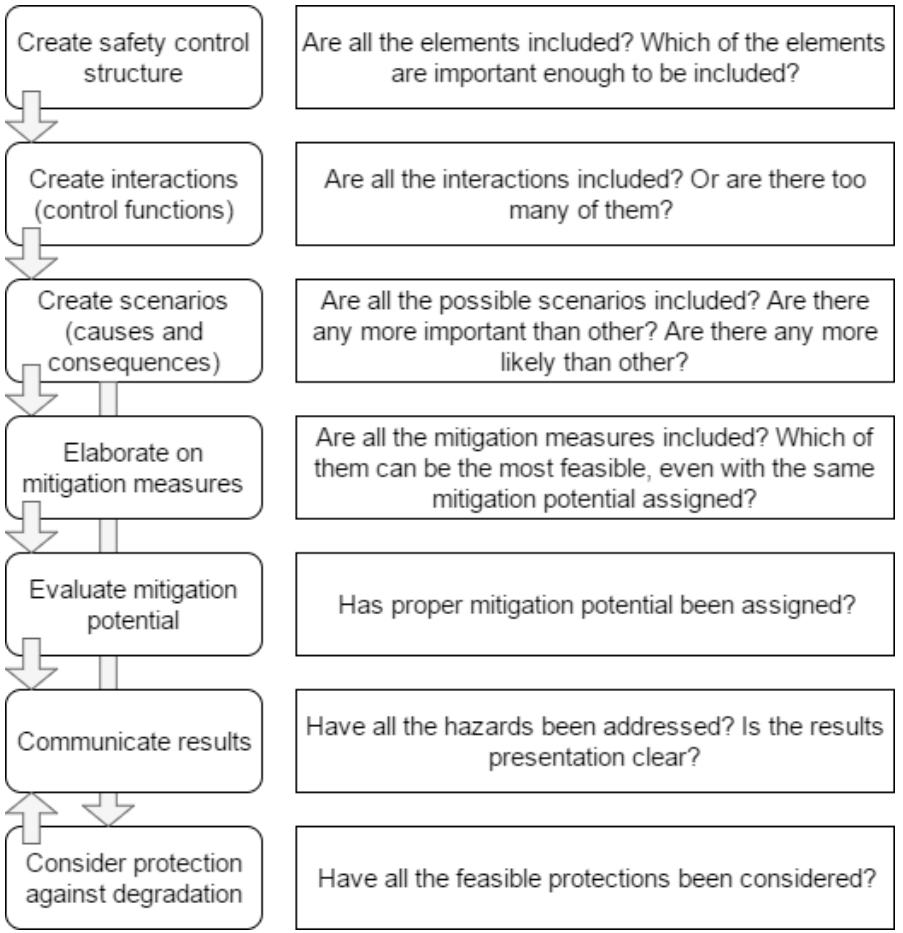
FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Systemic approach to assess the ways to control safety

System-Theoretic Process Analysis (STPA) is a method of assessing system's safety by analysing the interactions between its components and the ways in which those can be unsafe.

The nature of such interactions shall ensure that the system as a whole remains within safety limits.

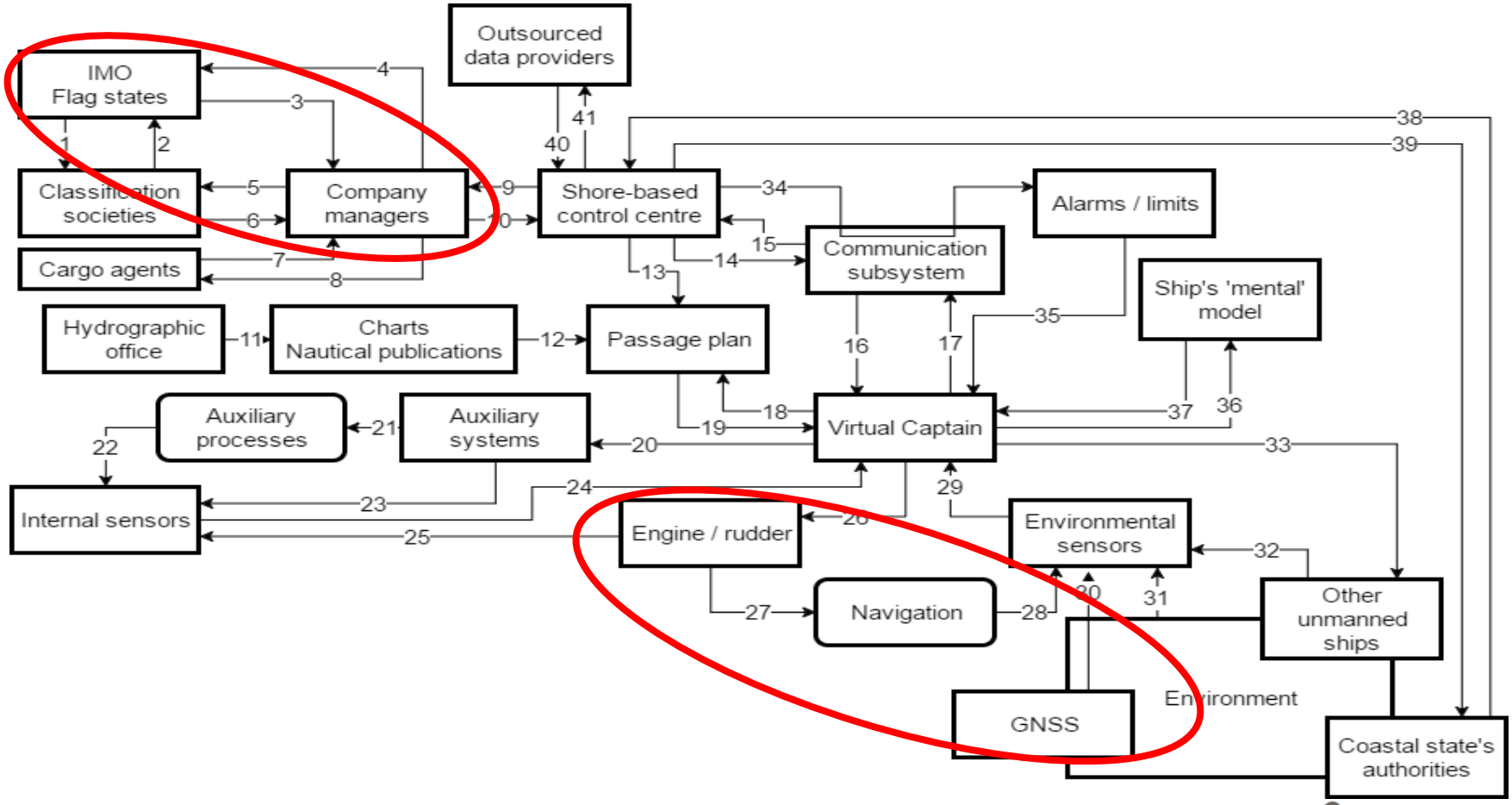
The aim is not to quantify the safety (mainly due to lack of data) but to ensure that it is controlled in proper manner.



NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

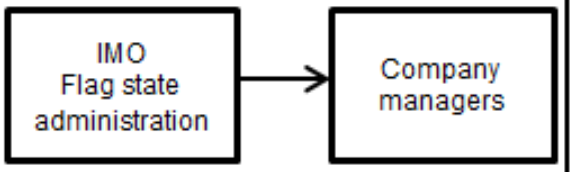
Systemic approach- safety control structure

Safety control structure for the proces of high-sea navigation of an autonomous merchant vessel

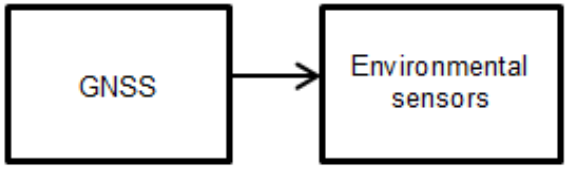


NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

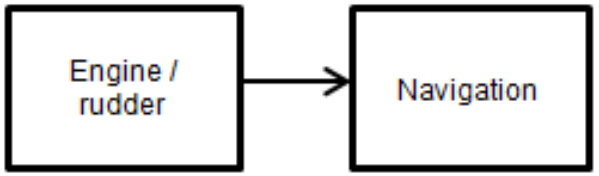
Systemic approach – safety control function

Control function number:	**3**				
Control function name:	*International legislation*				
Textual description:	Codes, legal acts and regulation governing various aspects of unmanned shipping				
Rationale:	International Maritime Organisation or flag states shall maintain regulatory control over shipping, including unmanned ships				
Potential for inadequacy:	***Control function is not provided***		***Unsafe control function is provided***		***Control function is provided in wrong time***		***Control function is provided for too short or too long***	
Consequences:	Improper regulatory supervision over unmanned shipping		Improper regulatory supervision over unmanned shipping		Legislation is issued before consulting interested parties			
Potential causes:	Need for regulation is not recognized; works are obstructed		Regulatory bodies have inadequate understanding of maritime industry		Pressure from society, intended misuse			
Feasible mitigation measures and potential	Workshops, conferences, lobbying	3	Workshops, conferences, lobbying	3	Procedures on legislation creation	3		
Protection against control degradation	Providing control function #4, proactive international and within-industry cooperation Accident/incident investigations		Providing control function #4, proactive international and within-industry cooperation Accident/incident investigations					

Systemic approach – safety control function

Control function number:	**30**				
Control function name:	*Sensing*				
Textual description:	Data provided by Global Navigation Satellite System				
Rationale:	The data is a vital information for the purposes of navigation process				
Potential for inadequacy:	***Control function is not provided***		***Unsafe control function is provided***	***Control function is provided in wrong time***	***Control function is provided for too short or too long***
Consequences:	Data on vessel's position, course and speed missing		Data on vessel's position, course and speed inaccurate		
Potential causes:	GNSS offline Vessel's antenna array unreliable		GNSS malfunction Vessel's antenna array malfunction		
Feasible mitigation measures and potential	Use of dead reckoning Use of eNavigation techniques	2 2	Use of dead reckoning Use of eNavigation techniques	2 2	
Protection against control degradation					

Systemic approach – safety control function

Control function number:	**27**	
Control function name:	*Actuation*	
Textual description:	Control over	
Rationale:	Main engine and rudder shall be capable of properly influencing vessel's movements	

Potential for inadequacy:	***Control function is not provided***		***Unsafe control function is provided***		***Control function is provided in wrong time***		***Control function is provided for too short or too long***	
Consequences:	Loss of control over vessel's movement		Loss of control over vessel's movement		Loss of control over vessel's movement		Loss of control over vessel's movement	
Potential causes:	Control functions #21,26 inadequate Machinery unreliable Consumables not provided		Control functions #21,26 inadequate Machinery having insufficient capacity Machinery improperly designed/installed		Control functions #21,26 inadequate Delays related to equipment's specificity and processes controlled Improper process management algorithms		Control functions #21,26 inadequate Improper process management algorithms	
Feasible mitigation measures and potential	Rigorous maintenance regime Redundant machinery Resilience-based design Procedures on consumables' management	3 3 1 3	Capacity surpluses by design Extensive testing	3 3	Implementation of leading performance indicators	3	Implementation of leading performance indicators	3

Systemic approach to assess the ways to control safety

A total of 47 control functions have been analysed with respect to their position within the system structure, potential scenarios leading to their inadequacy and consequences of such.

Furthermore, potential ways of mitigating such inadequacies were elaborated and evaluated by assignment of the mitigation potential.

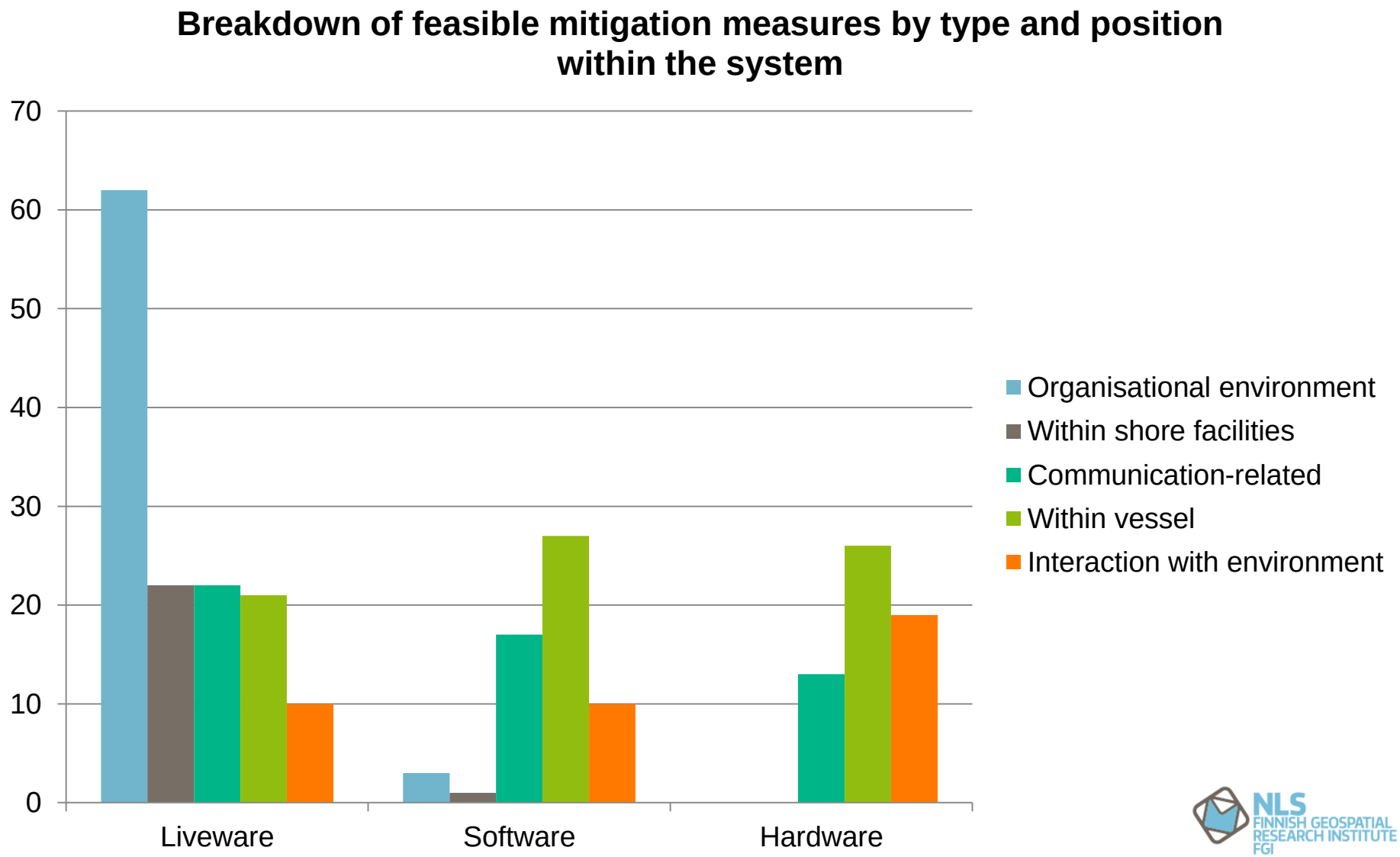
A total of 253 recommendations on mitigation measures implementation have been elaborated, each of them pertaining to one of three groups:

- liveware,
- software,
- hardware.

By 'liveware' we understand all organisational, legal and operational factors in which a human plays a major and direct part.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Systemic approach – types of mitigation measures



NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

Systemic approach – uncertainty assessment of the model

Uncertainties pertaining to the outcome of the study come as a result of the unmanned shipping technology being in its infancy. No empirical data or reliable models of such ships' safety performance is available.

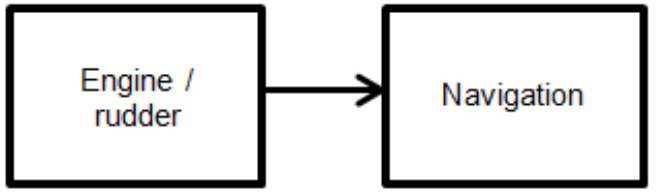
The subjective uncertainty assessment, borrowed from the risk analysis, and applied in system-theoretic approach tends to reflect the analyst's level of background knowledge in each of five categories:

		Uncertainty magnitude		
		Significant	Moderate	Minor
Category	Phenomena	Low level or no understanding	Medium level of understanding	High level of understanding
	Model	No basis for models or models give poor predictions	Some basis for models, level of simplifications adopted varies across the model; alternative hypotheses exist	Strong basis for the models, which give good predictions
	Assumptions	Poor justifications for the assumptions made, oversimplifying the analysed phenomena	Reasonable justifications for the assumptions made, although simplifying the analysed phenomena	Seen as reasonable
	Data	Not available or reliable	Data of varying quality is available	Much reliable data is available
	Consensus	Lack of consensus	Various views exist among experts	Broad agreement among experts

Flage, R. & Aven, T. 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. Reliability & Risk Analysis: Theory & Application 2(13), 9-18.

NLS FINNISH GEOSPATIAL RESEARCH INSTITUTE FGI

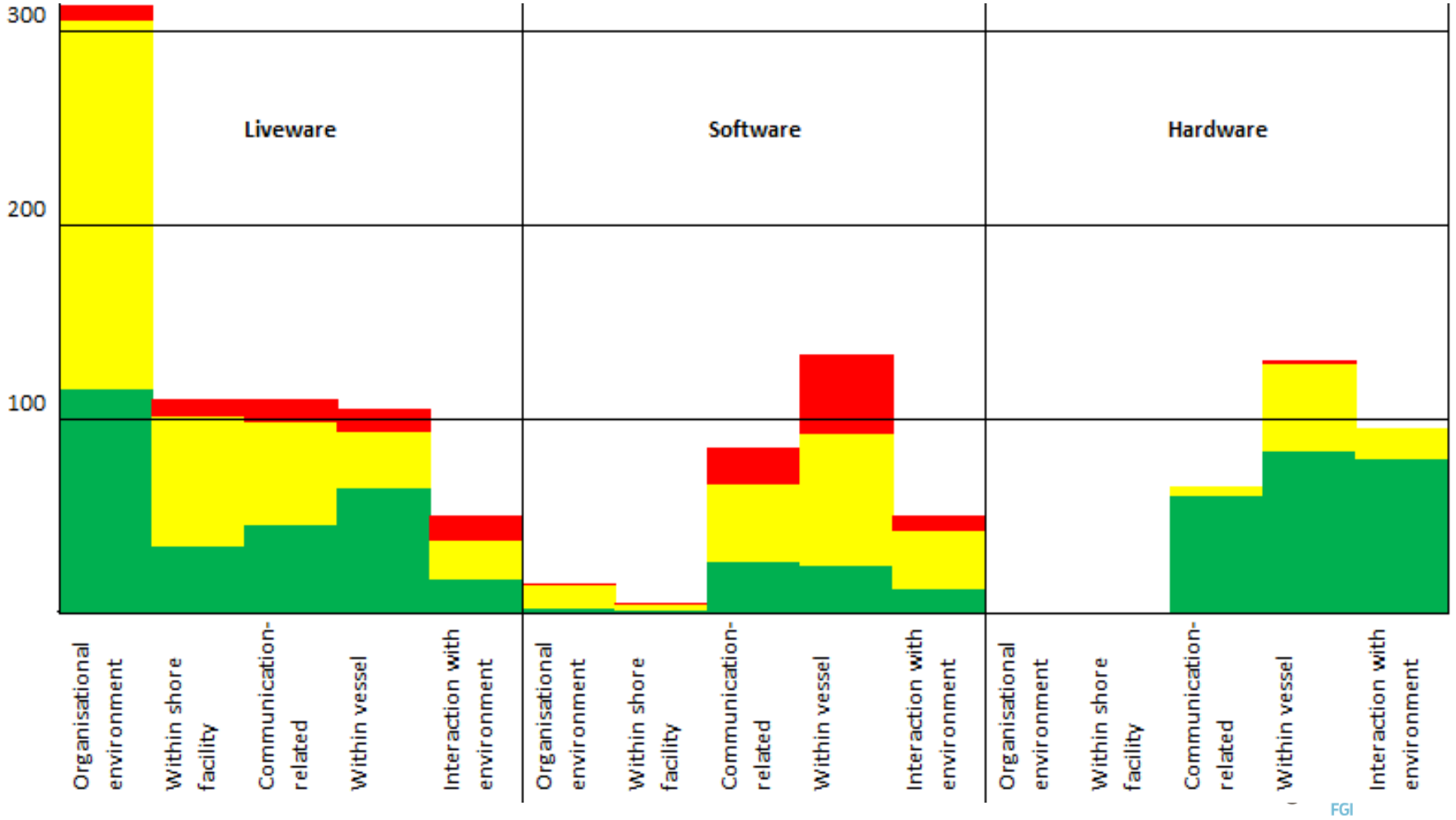
Systemic approach – uncertainty assessment of the model

Control function number:	27								
Potential causes:	Control functions #21,26 inadequate Machinery unreliable Consumables not provided		Control functions #21,26 inadequate Machinery having insufficient capacity Machinery improperly designed/installed		Control functions #21,26 inadequate Delays related to equipment's specificity and processes controlled Improper process management algorithms		Control functions #21,26 inadequate Improper process management algorithms		
Feasible mitigation measures and potential	Rigorous maintenance regime	3	Capacity surpluses by design	3	Implementation of leading performance indicators	3	Implementation of leading performance indicators	3	
	Redundant machinery	3	Extensive testing	3					
	Resilience-based design	1							
	Procedures on consumables' management	3							

Category		Uncertainty magnitude: Significant	Moderate	Minor
	Phenomena	Low level or no understanding	Medium level of understanding	High level of understanding
	Model	No basis for models or models give poor predictions	Some basis for models, level of simplifications adopted varies across the model; alternative hypotheses exist	Strong basis for the models, which give good predictions
	Assumptions	Poor justifications for the assumptions made, oversimplifying the analysed phenomena	Reasonable justifications for the assumptions made, although simplifying the analysed phenomena	Seen as reasonable
	Data	Not available or reliable	Data of varying quality is available	Much reliable data is available
	Consensus	Lack of consensus	Various views exist among experts	Broad agreement among experts

Systemic approach – uncertainty assessment of the model

Breakdown of the uncertainties by its magnitude, type of relevant mitigation measure and position within the system



Conclusions

- Unmanned vessels can potentially reduce the likelihood of maritime accidents. Meanwhile, their consequences can become more serious.
- This can be attributed to the fact that failure propagation could not be properly safeguarded against as there will be no crew to control the damage.
- Therefore, certain safety recommendations must be created and implemented. Concurrent application of various safety assessment methods can be of use in this case.
- Feasibility of certain solutions is burdened with significant uncertainties – more research is required.
- Unfortunately, the present stage of technology development does not allow for highly-detailed analysis. However, this may change in the nearest future.

Thank you for your attention

For more information, please contact:

Jakub Montewka, DSc (Tech.)
Specialist Research Scientist
Intelligent Mobility and Geospatial Computing Group
Geodeetinrinne 2; FI-02430 Masala
FINLAND

Tel +358 50 5916740
E-mail jakub.montewka@nls.fi, jakub.montewka@aalto.fi
www https://www.researchgate.net/profile/Jakub_Montewka