Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping

Montewka J., Wróbel K., Heikkila E.,
Valdez Banda O., Goerlandt F., Haugen S.

Gdynia Maritime University, Poland
VTT Technical Research Centre of Finland Ltd, Tampere, Finland
Aalto University, Espoo, Finland
Dalhousie University, Halifax, Canada
NTNU Trondheim, Norway

PSAM 14
Probabilistic Safety Assessment and Management
16–21 September 2018 • UCLA Meyer & Renee Luskin Conference Center, Los Angeles, CA

Agenda

1. Introduction

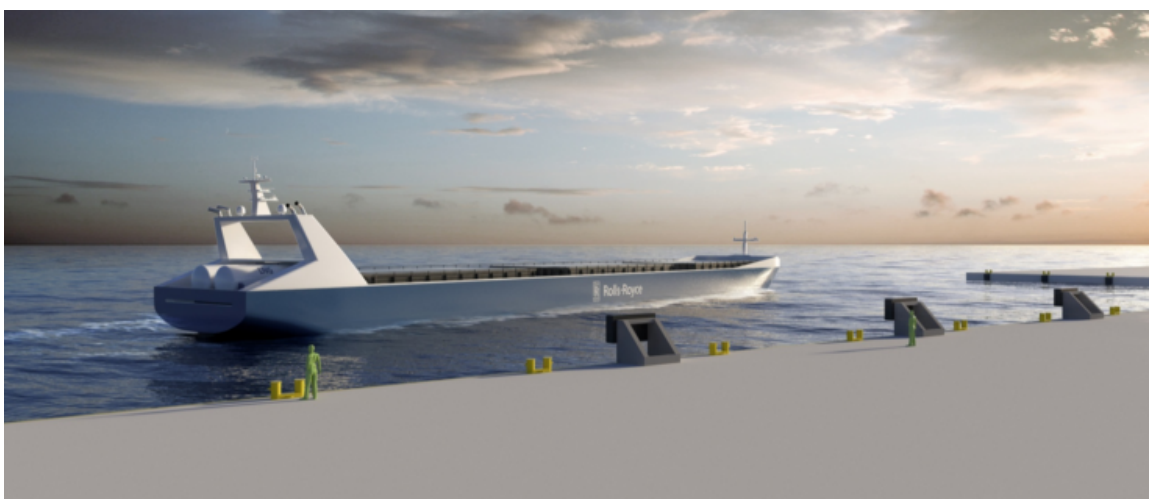
2. Summary and discussion of the existing methods
    1. Risk-informed design (Formal Safety Assessment, Goal-based Standards)
    2. System theoretic process analysis
    3. Safety case approach

3. Conclusions

Background, aim and scope

- Safety of maritime transportation is governed by global and local codes and practices, and a distillation of past experience. It is highly prescriptive world.

- Such approach suffices for standard ships, however for highly innovative solutions, like autonomous ships, another way of ensuring safe operations is needed.



Background, aim and scope

- Another approach is based on qualitative method, such as System-Theoretic Process Analysis (STPA).
- Safety therein results from enforcing adequate constraints (control actions) on the interactions between system's components.
- Safety of the system is not calculated, but ways to ensure it are sought.

Background, aim and scope

- Therefore in this paper we discuss selected methods suitable for safety assessment and quantification of transportation systems including:
    - risk assessment,
    - system theoretic process analysis,
    - safety case approach.

- Challenges and opportunities of those approaches are highlighted and the recommendations are given regarding the application areas of the methods.

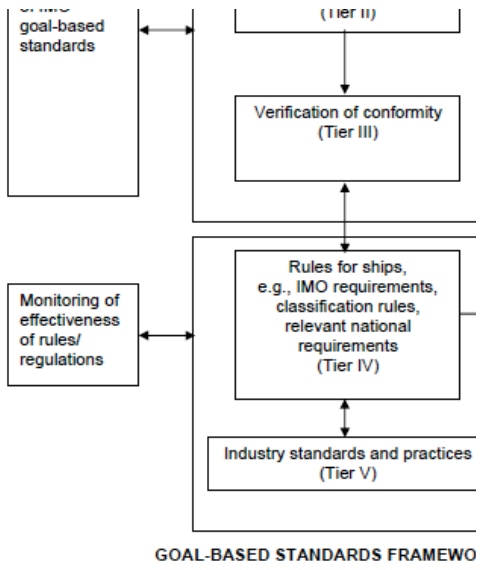
Methods: FSA, GBS

- International Maritime Organization offers solutions for proactive safety assessment and management called Formal Safety Assessment and Goal-based Standards.
- Therein safety is measured through a concept of risk,
- A system is considered safe as long as the calculated risk value falls within the acceptable risk limits.
- The need of quantitative risk estimates is challenging.

Formal Safety Assessment - FSA

System description Scope	•What is the purpose of the analysis? •Which parts of the system are analyzed?
Hazard Identification	**•What can go wrong?** •Scenarios
Risk Analysis	**•How likely is it?** •Probabilities
Risk control options	**•What can we do about it?** •How much does it help?
Cost-benefit analysis*	**•At what cost?*** •Do the benefits outweigh the costs?*
Recommendations	•Decision criteria •Prioritized actions

Goal-based standards - GBS



Methods: FSA, GBS

- The Guideliness for FSA defines risk as a follows:

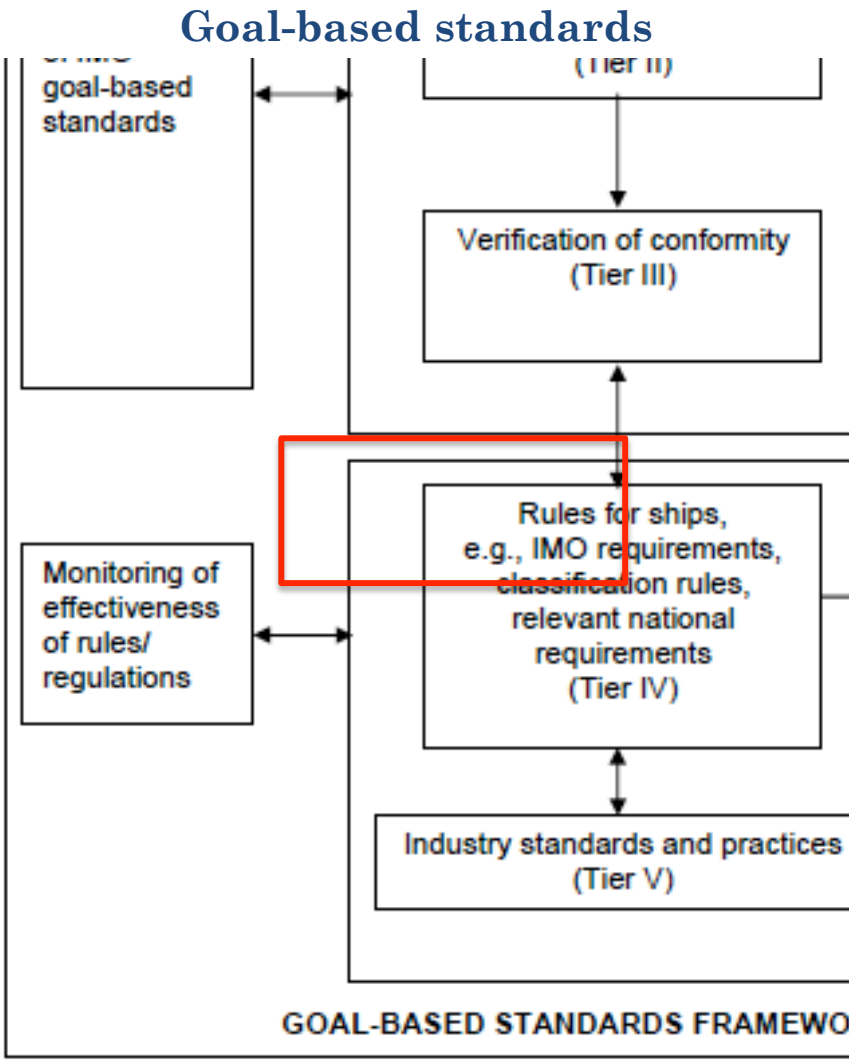
R=PxC

- It is not clear how to express uncertainty and its effects on risk metrics and risk control options?
- Quantitative approach is strongly preferred, precise risk esitmates are sought.
- Interpreting risk simply as this combination, may lead to misconception, that the risk is just a number, divorced from the scenario of concern and available background knowledge.
- This in turn may lead to the loss of relevant information needed for risk management.

- PxC definition of risk dominates the field, despite the existence of other, more flexible and broader definitions in other domains (e.g. oil and gas).

Methods: FSA, GBS

- In the context of GBS the concept of risk is used at the **stage of verification of conformity** (Tier III).
- The risk level of a given ship design is confronted with the allowed risk levels as anticipated by the rules (Tier IV).
- The tolerable, intolerable and ALARP risk levels are defined by the the relevant stakeholders like IMO, authorities or classification societies.

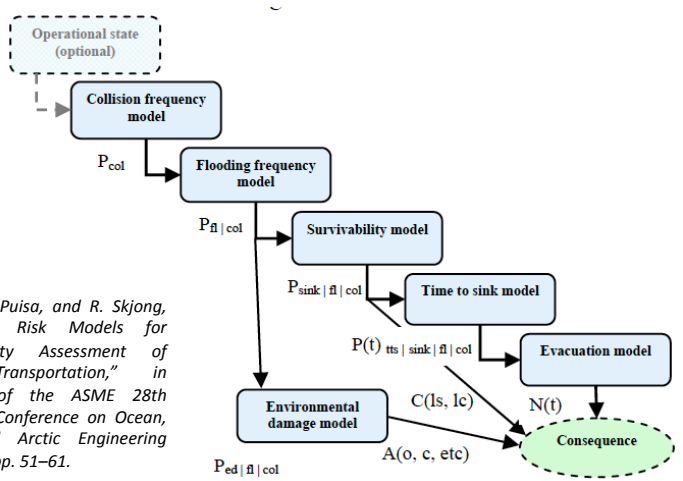


Methods: FSA, GBS

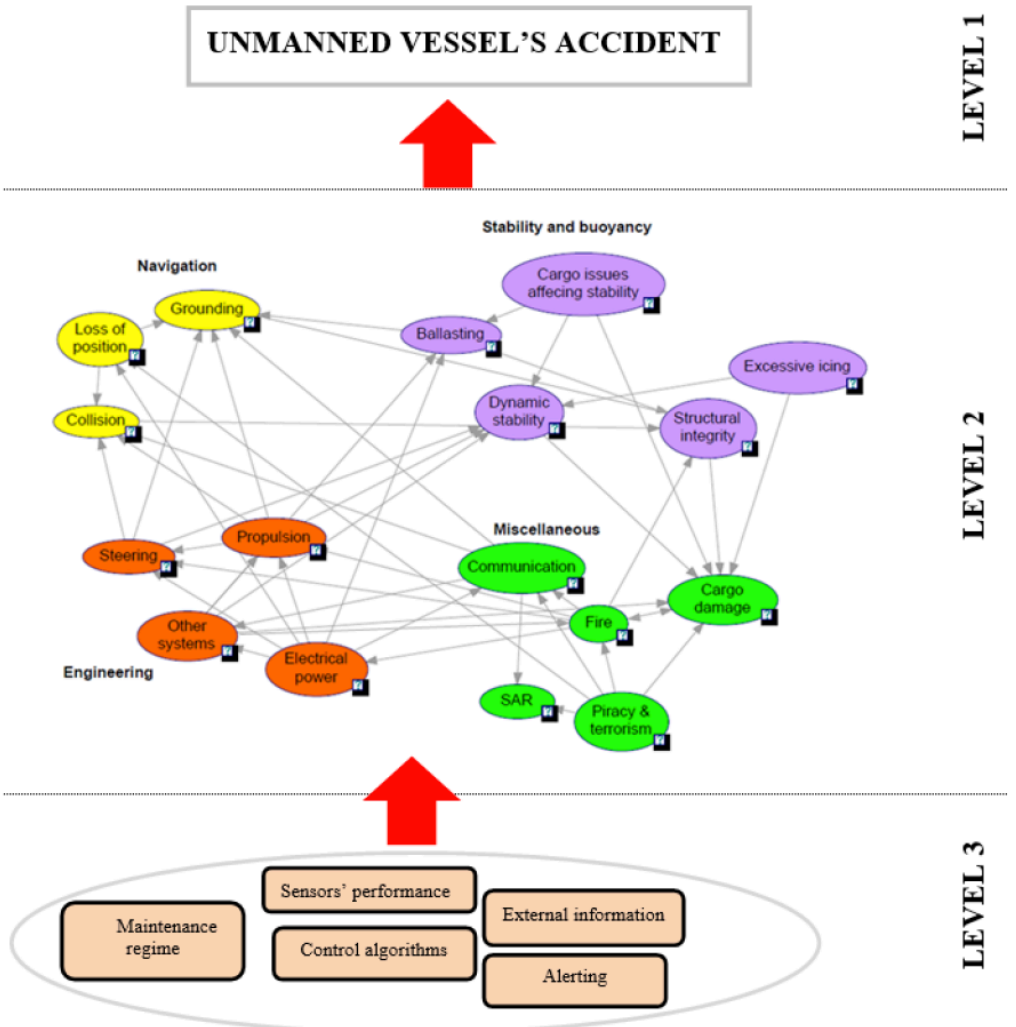
- In many risk analyses, one sees that a lot of effort is put into producing as "accurate" risk numbers as possible. In fact, they are often only precise, but not accurate.
- However, it is futile to calculate high-precision values in the risk analysis if other parameters essentially are "guesstimates" made by the analyst.
- In the extreme cases, the numbers obtained from databases and analysis are considered "the ultimate truth" about the probability of an accident in the analysed area, without proper reflection of the context and background knowledge.

Methods: FSA, GBS

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

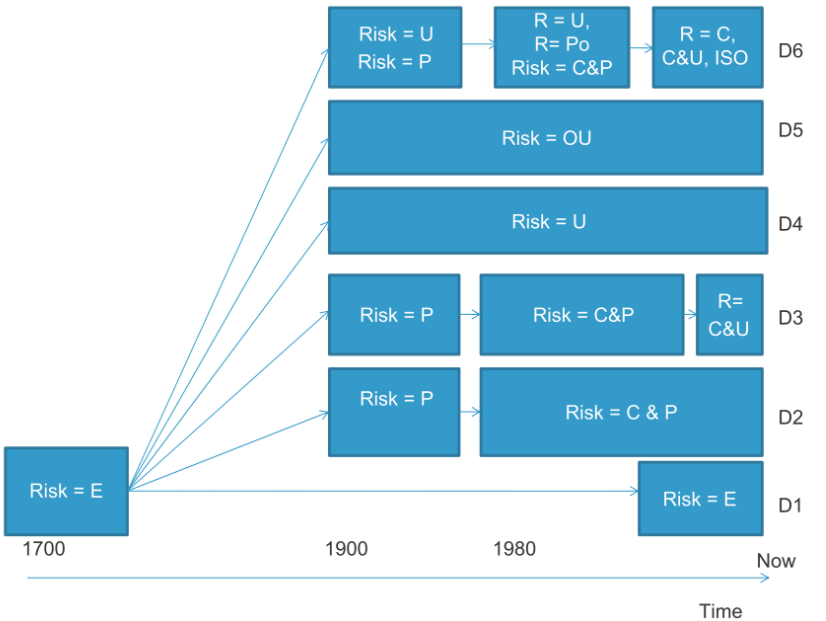


E. Vanem, R. Puisa, and R. Skjong, "Standardized Risk Models for Formal Safety Assessment of Maritime Transportation," in Proceedings of the ASME 28th International Conference on Ocean, Offshore and Arctic Engineering OMAE, 2009, pp. 51–61.

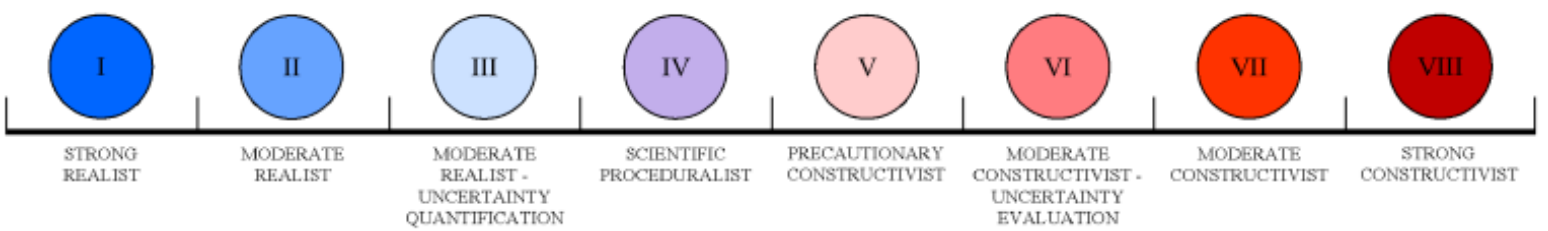


Discussion – FSA, GBS

- A wider concept of risk should be introduced to the field.
- Various scientific approaches to risk exist, depending on the available background knowledge, utilizing the available sources of data and knowledge. These should be utilized.
- Recent shift in risk paradigm in oil&gas industry should be a sign for maritime.

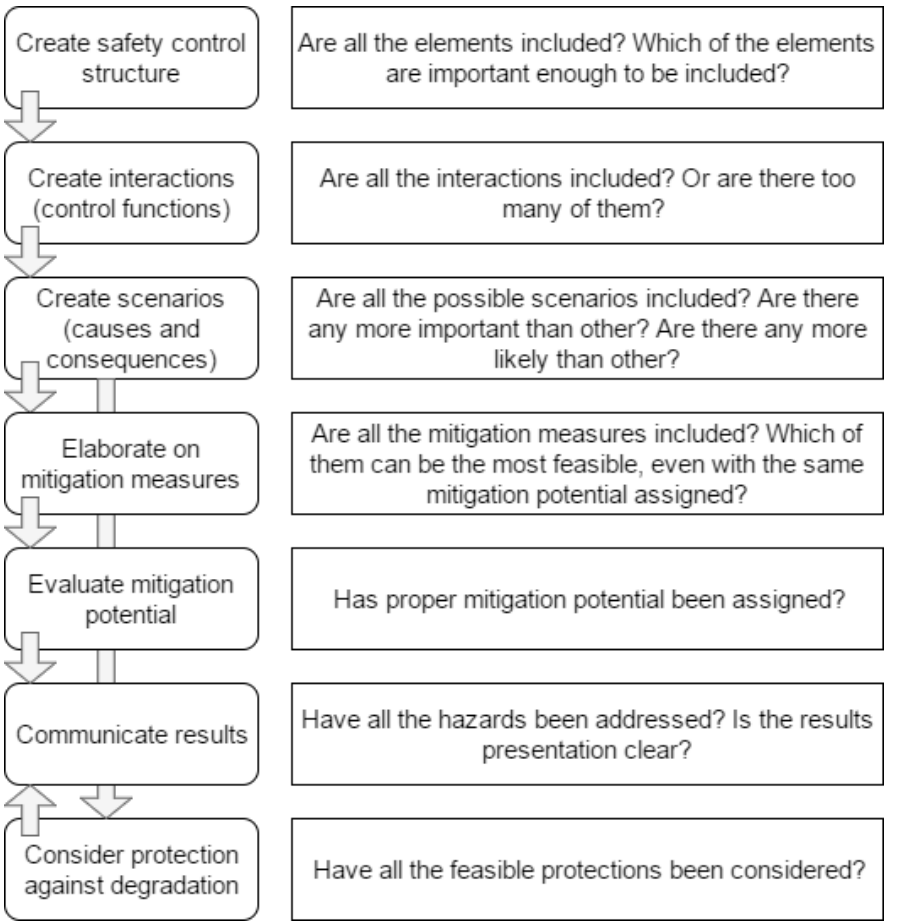


Aven, T. 2012. The risk concept – historical and recent development trends. Reliability Engineering and System Safety 99:33-44

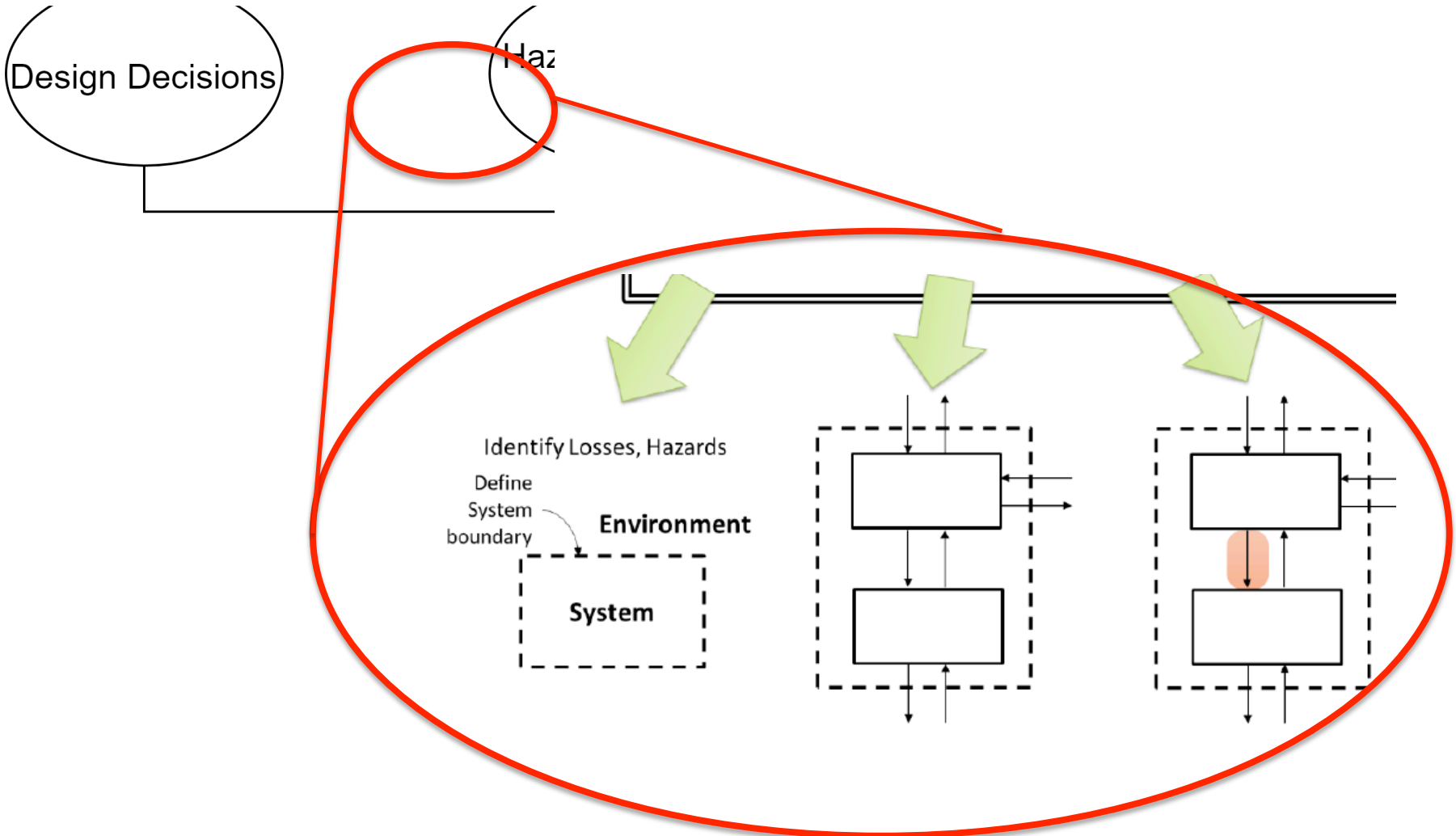


Methods: STAMP / STPA

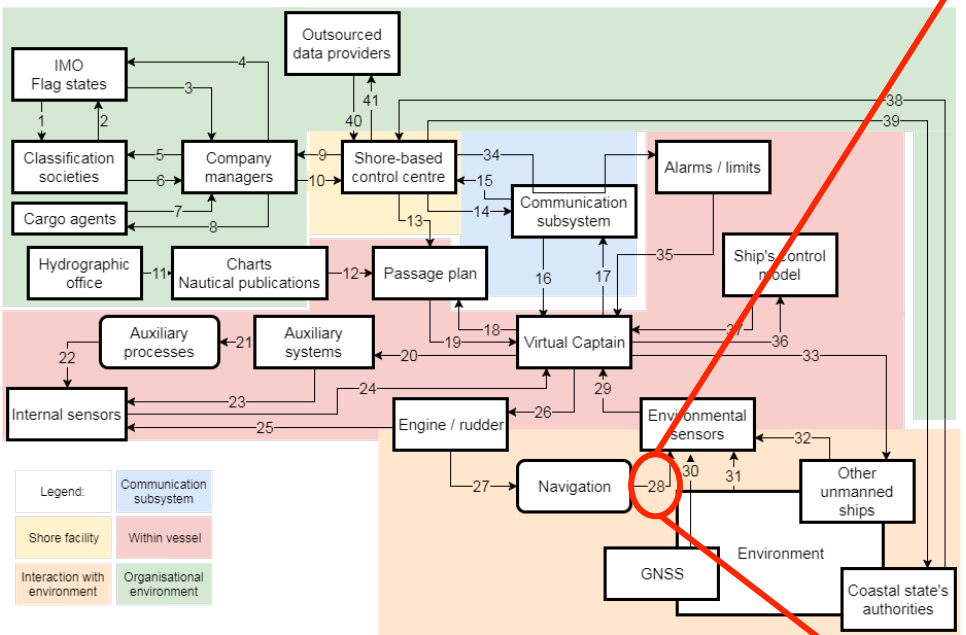
- System-Theoretic Process Analysis (STPA) is a method of assessing system's safety by analysing the interactions between its components and the ways in which those can be unsafe.
- The nature of such interactions shall ensure that the system as a whole remains within safety limits.
- The aim is **not to quantify the safety** (mainly due to lack of data) **but to ensure that it is controlled in proper manner**.



Methods: STAMP / STPA



Methods: STAMP / STPA



Control action number:	**28**	Navigation →	Environmental sensors

Control action name:	*Sensing*
Type:	Feed
Textual description:	Examination of processes' status
Rationale:	Vessel's course and speed as well as other elements of her movement should be measured for VC to make informed decisions

Hazards resulting:	1.1 Vessel violates minimum CPA with another ship 1.2 Vessel enters a No Go Area 1.3 Vessel improperly interacts with other man-made objects 2.1 Vessel enters a No Go Area 2.2 Propulsion/steering gear operational parameters cannot be maintained 2.4 Vessel's navigational capabilities are severed by weather conditions 2.5 Vessel does not meet stability criteria 3.1 Vessel's cargo is not loaded/stowed properly 3.2 Vessel is unable to maintain proper cargo stowage conditions 4.3 Vessel does not meet fire safety precautions 5.2 Vessel is unable to maintain proper fuel combustion parameters 6.2 Vessel contributes to delay of other ships' traffic 6.3 System does not meet international, classificatory or national regulations 6.5 System's interaction with other assets (including unmanned vessels) leads to the emergence of any of above

Potential for inadequacy:	***Control action is not provided***	***Unsafe control action is provided***	***Control action is provided in wrong time***	***Control action is provided for too short or too long***
Consequences:	Vessel's motion components are not known	Vessel's motion components are measured improperly	Vessel's motion components are measured with delay	
Potential causes:	Sensors unreliable Required parameter cannot be measured	Sensors' malfunction Parameters outside sensors' working range Sensor's accuracy insufficient	Non-continuous characteristics of sensors' operation Sensors' idleness due to measured phenomenon's specificity	
Feasible mitigation measures and potential	Redundant or highly-reliable sensors Indirect measurement	Redundant or highly-reliable sensors Implementation of wide-range sensors	Use of highly-sensitive sensors	
Protection against control degradation	Constant search for and installation of improved sensors Use of leading indicators on sensors' performance	Constant search for and installation of improved sensors Use of leading indicators on sensors' performance	Constant search for and installation of improved sensors Use of leading indicators on sensors' performance	

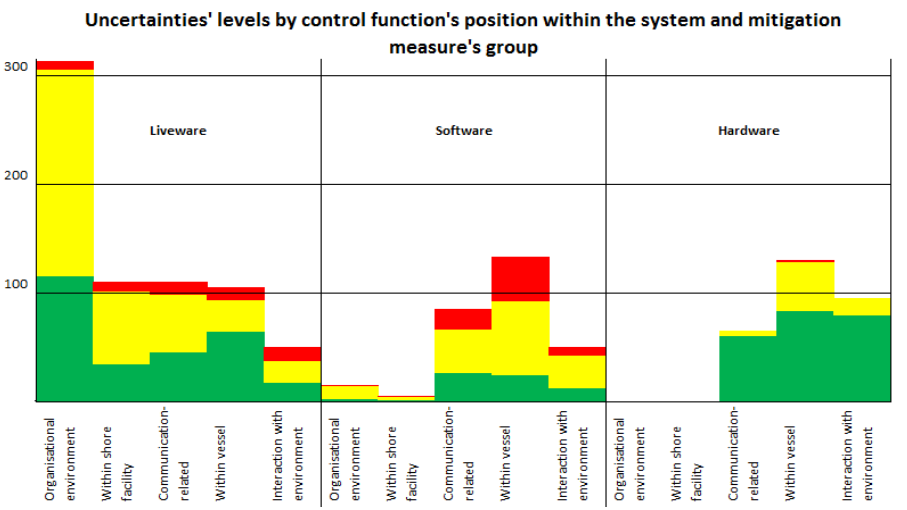
Wróbel, K., Montewka, J., & Kujala, P. (2018). System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Engineering, 152, 334–345.

Discussion - STPA

- 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.

		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.

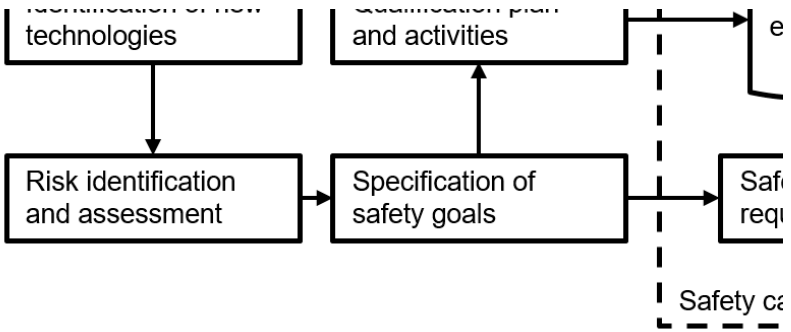


Methods: safety case approach

- The goal-based safety case approach is a proposed extension to the regular safety qualification methodologies to help in structuring the results of qualification activities and especially in enabling communication between the different stakeholders involved in the safety design and qualification processes.
- In this approach, the safety requirements (represented as goals) and safety evidence (data created in the actual qualification activities) are presented together in a visual manner as a structured safety case. This provides a link showing which evidence items are provided to demonstrate the fulfillment of each of the safety goals.
- The structure of safety goals is a living documentation that is updated throughout the design and qualification processes.

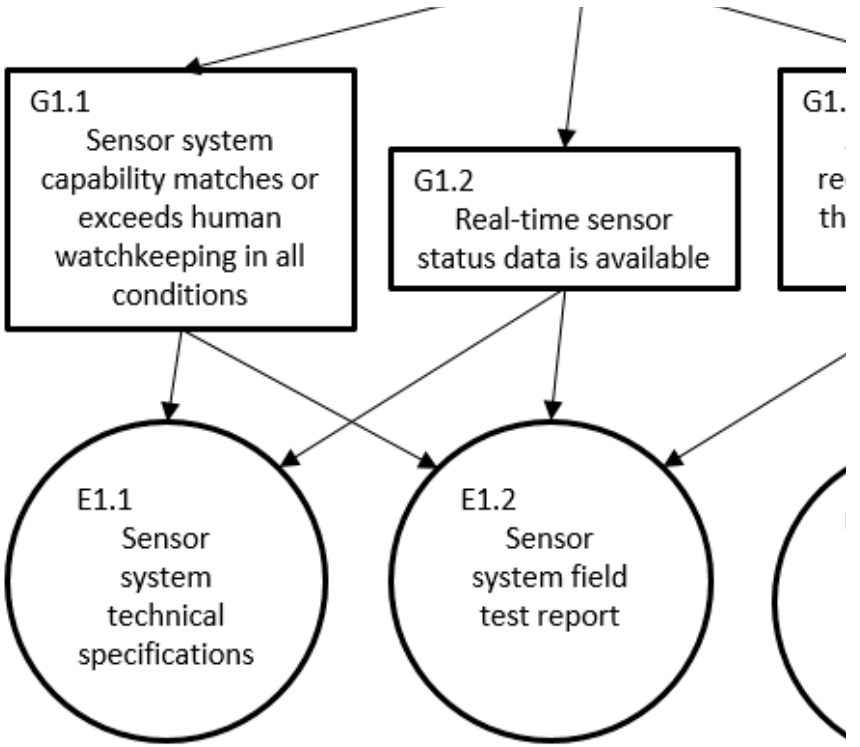
Methods: goal-based safety case approach

A safety qualification procedure, resulting in safety argumentation documented as structured safety case.



Heikkilä E., Tuominen R., Tiusanen R., Montewka J., Kujala P. 2017. "Safety Qualification Process for an Autonomous Ship Prototype - a Goal-Based Safety Case Approach." In Marine Navigation, pp.365–70. CRC Press. doi:doi:10.1201/9781315099132-63.

A simplified example of how the safety goals and evidence can be represented in the case of an autonomous ship sensor system.



Discussion – safety case

- The major advantages of the method are in the communicative power of the visual representation of safety goals and evidence, making the link between these easily comprehensible.
- This enables efficient communication regarding safety between the different stakeholders, and enables a faster approval of new technologies for autonomous shipping.
- The methodology is mainly designed with the communicational aspect in mind, and thus provides no direct tools for prioritizing the safety goals based on their safety impact.
- Neither does it directly provide tools for assessing the probabilities or uncertainties regarding the fulfillment of the goals.
- The methodology, however, is new to the maritime sector and further case applications are needed to fully consider its benefits.

Conclusions

- Goals-based and risk-informed approaches give flexibility in development of novel solutions, at the same time as retaining consistent and acceptable risk levels also for new technology.

- However a more flexible perspective on risk is needed, where in particular the aspect of background knowledge/uncertainty is incorporated, to give to decision-makers better basis for making sound decisions.

- New safety and risk analysis methods are better suited for analysing increasingly complex systems, with increased use of sensors, software, communication between ships and between ship and shore, very different demands on the humans involved etc.

- STPA may be one of such methods, but it is crucial to understand the system being analysed and its characteristics before committing to specific risk or safety analysis methods. Both method development and more guidance on choice of methods and combinations of methods is required.

Thank you for your attention.

For more information, please contact:

Jakub Montewka, DSc (Tech.)
Associate professor
Dept. of Transport and Logistics
Gdynia Maritime University
POLAND

Tel. +48 732666078
E-mail j.montewka@wn.am.gdynia.pl
www https://www.researchgate.net/profile/Jakub_Montewka

PSAM 14

Probabilistic Safety Assessment and Management

16–21 September 2018 • UCLA Meyer & Renee Luskin Conference Center, Los Angeles, CA

UCLA LUSKIN CONFERENCE CENTER