A method for uncertainty assessment and communication in safety-driven design. A case study of unmanned merchant vessel

Krzysztof Wróbel

Jakub Montewka

5th European STAMP Workshop

14th Sep 2017 Reykjavik

k.wrobel@wn.am.gdynia.pl

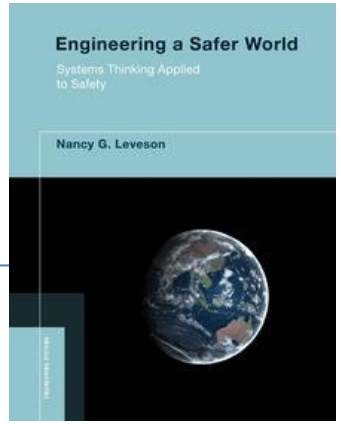
Agenda

Intro

1. Unmanned shipping
2. Assessing safety of unmanned vessel - a non-existing system
3. Uncertainties
4. Method of uncertainties' assessment and communication
5. Results

Conclusions

Introduction



System-Theoretic Accident Model and Process (STAMP) strikes as a novel and improved way of looking into systems' safety. It is so amazingly perfect in describing all the interactions and concluding on hazard mitigation measures that one may ask:

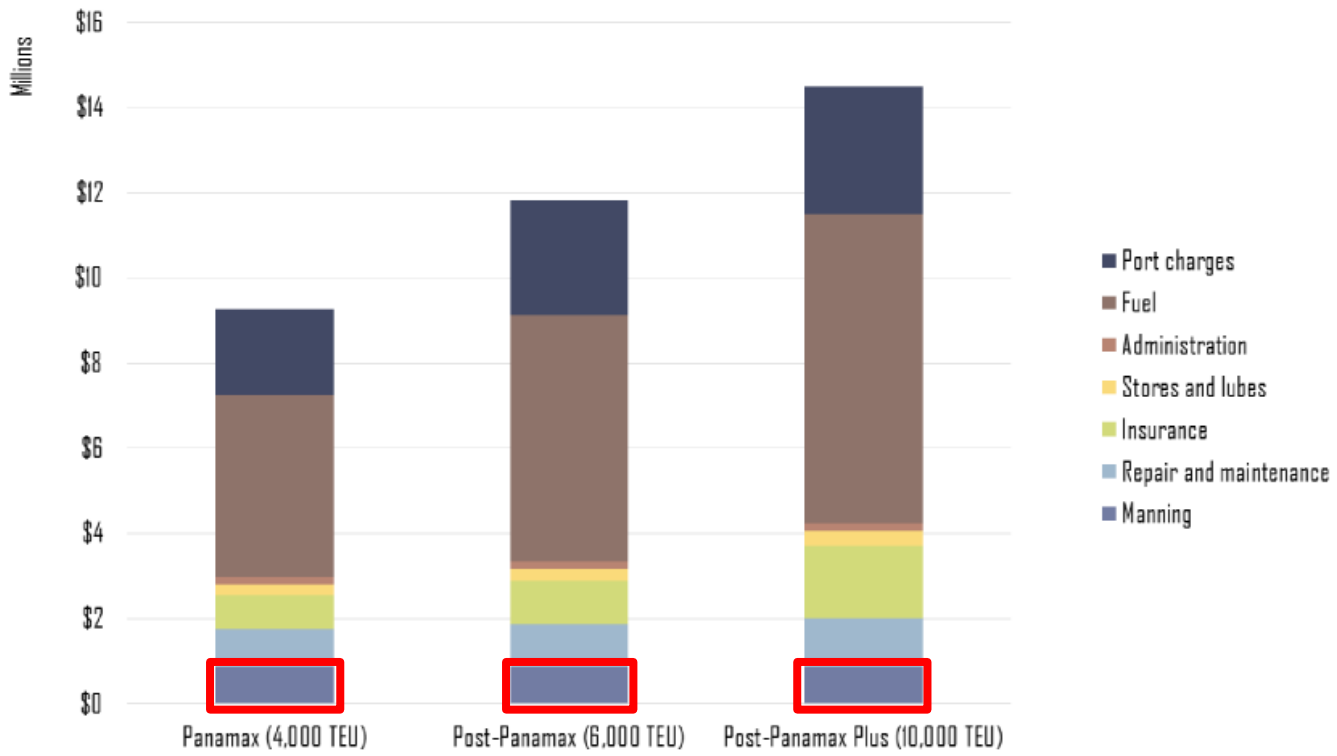
Where is the catch?

One of them is an uncharted territory of uncertainties treatment.

The study is based on unmanned merchant vessels' case.

https://mitpress.mit.edu/books/engineering-safer-world

Unmanned shipping

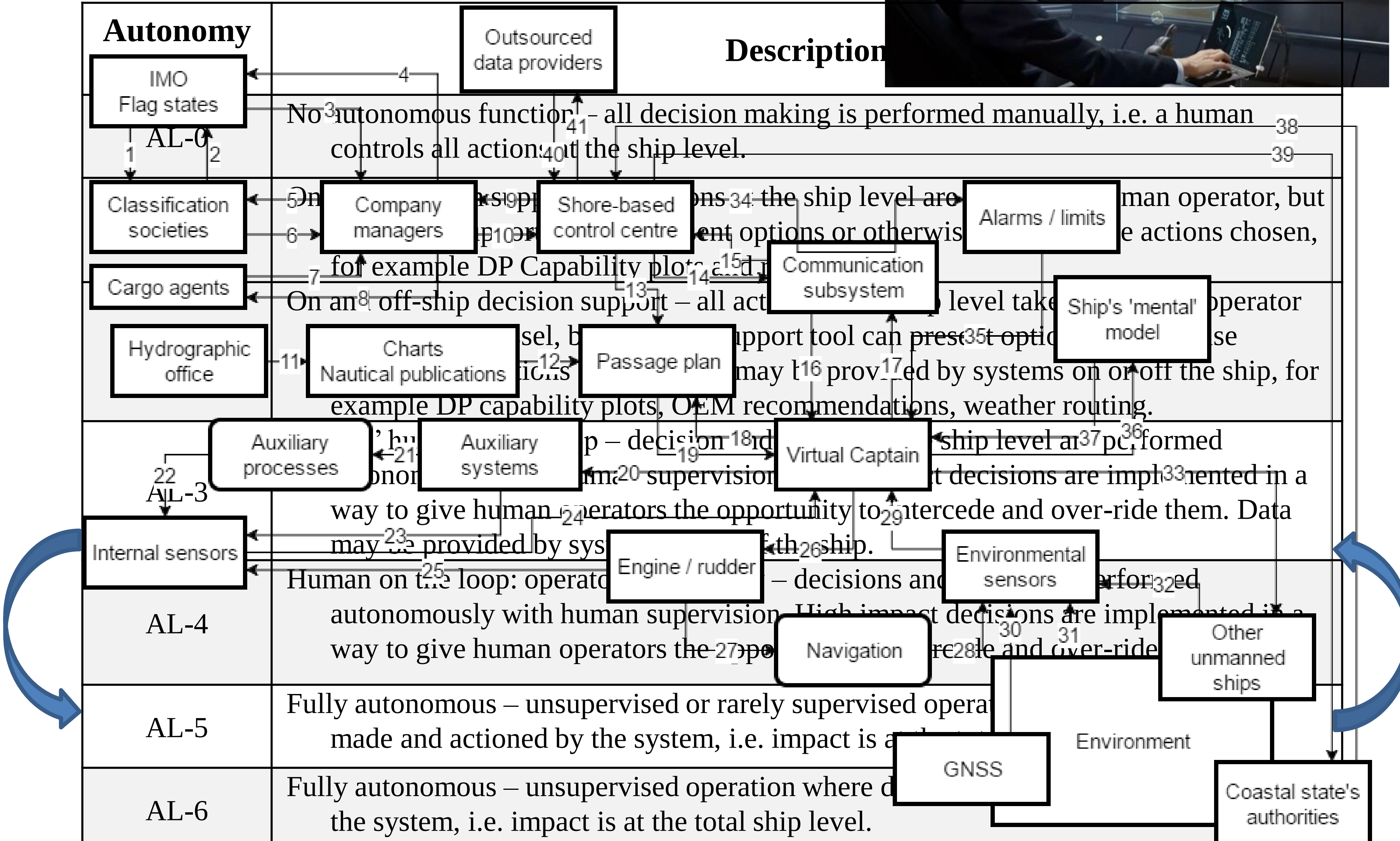


Although manning represents a fraction of total shipping costs, savings can still be significant.

Drewry Shipping Consultants Ltd., does not include amortization

Unmanned shipping

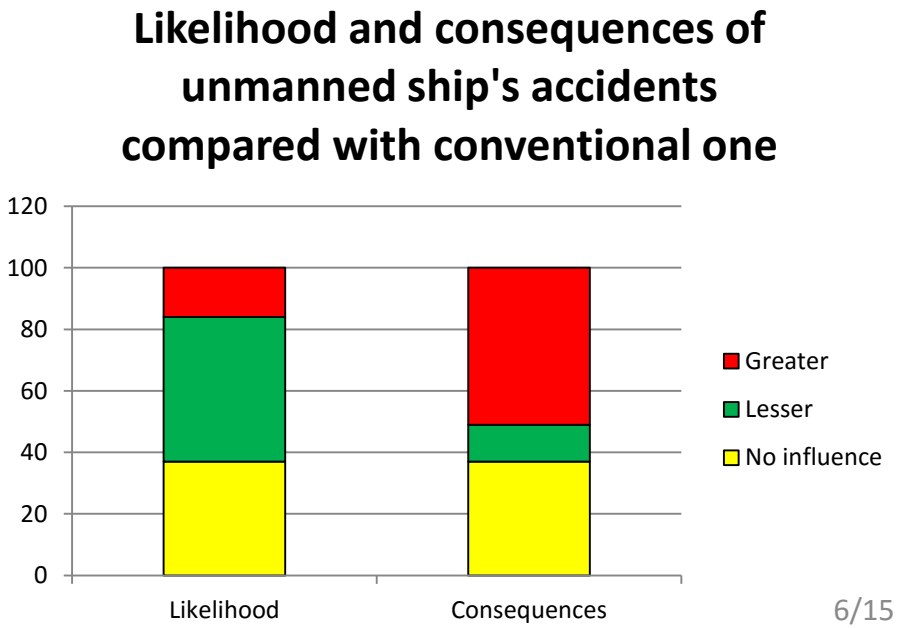
Autonomy	Description
AL-0	No autonomous function – all decision making is performed manually, i.e. a human controls all actions at the ship level.
[illegible]	On[illegible] the ship level are [illegible] man operator, but [illegible] ent options or otherwis[illegible] e actions chosen, for example DP Capability plots a[illegible]
[illegible]	On an[illegible] off-ship decision support – all act[illegible] level take[illegible] operator [illegible] sel, b[illegible] upport tool can prese[illegible] t optio[illegible] se [illegible] may b[illegible] provided by systems on or off the ship, for example DP capability plots, OEM recommendations, weather routing.
AL-3	[illegible] p – decision[illegible] ship level are performed [illegible] nomo[illegible] supervision[illegible] t decisions are implemented in a way to give human operators the opportunity to intercede and over-ride them. Data may [illegible] provided by sys[illegible] f the ship.
AL-4	Human on the loop: operat[illegible] – decisions and [illegible] rformed autonomously with human supervision. High impact decisions are implemented in a way to give human operators the [illegible] e and over-ride [illegible]
AL-5	Fully autonomous – unsupervised or rarely supervised operat[illegible] made and actioned by the system, i.e. impact is a[illegible]
AL-6	Fully autonomous – unsupervised operation where d[illegible] the system, i.e. impact is at the total ship level.



Unmanned shipping

Although unmanned ships may help reduce some hazards to shipping, they will create other issues related to:

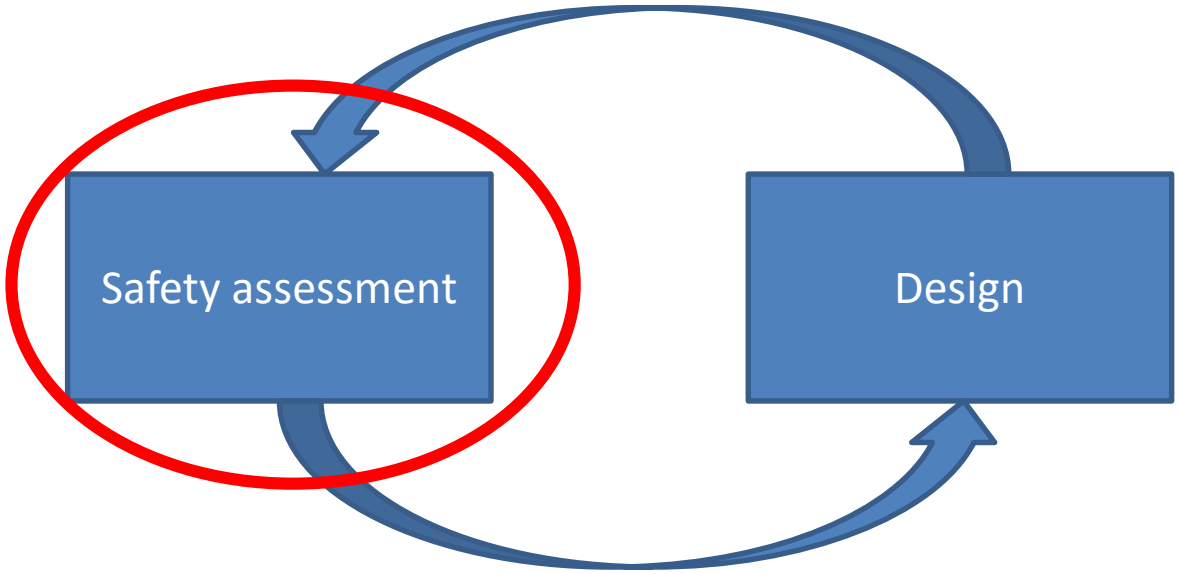
- Remote control;
- Autonomous control;
- Equipment reliability;
- Artificial situational awareness;
- Inability of manual intervention;
- Cargo conditioning and care;
- Salvage;
- Cyber-security.



http://www.heavyliftnews.com/
http://www.wersm.com/
Wróbel, K. *et alia*.: Towards the assessment of potential impact of unmanned vessels on maritime transportation safety

Assessing safety of a non-existing system

Safety-guided design principles treat on formulating safety recommendations for systems being developed.



The unmanned ship is in such an early design phase that nothing about can be said for sure. If so, how can we assess the safety of the system? How to produce safety recommendations?

Uncertainties

System-theoretic methods are said to improve hazard analysis process by providing more insighful look at the systems in question.

Moreover, as safety assessments are an input to decision-making, the designers shall be made aware of the strength of argument supporting particular statements. The uncertainties should therefore be

1. Reduced to as far as possible,
2. Communicated as accurately as possible.

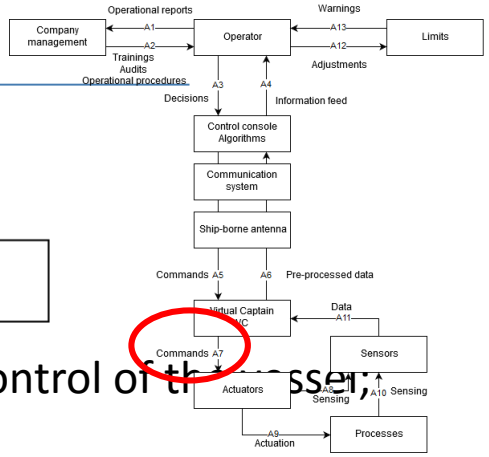
To address (2), we suggest a method of qualitatively assessing and communicating uncertainties pertaining to safety recommendations' formulation.

Method of uncertainties assessment and communication

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

Inspired by: Flage, R. & Aven, T.: Expressing and communicating uncertainty in relation to quantitative risk analysis

Results



	Significant	Moderate	Minor
Phenomena			
Process Model			
Assumptions			
Data			
Consensus			

Hypothesis:

H1. Both human operator and Virtual Captain are in control of the vessel;

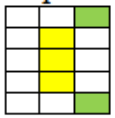
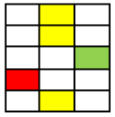
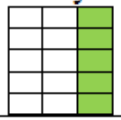
H2. Neither of above is in control of the vessel;

H3. Improper of above [illegible] of the vessel.

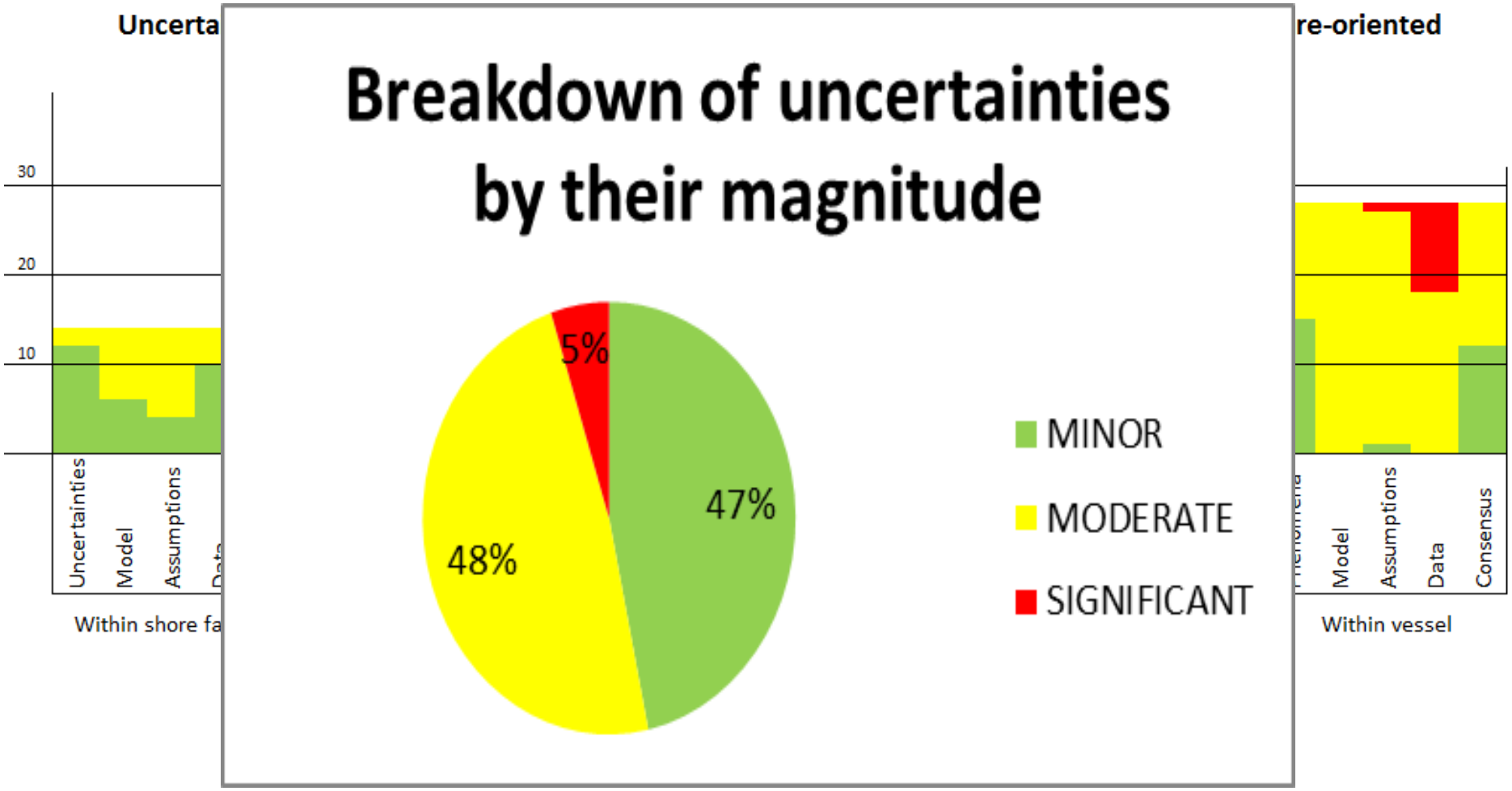
Number	Description	Control action is not provided	Unsafe control action is provided	Control action is provided in wrong time or sequence	Control action is provided for too short or too long
A7 Commands	Results in	VC does not relay mode transition command to actuator	[illegible]mand relayed to [illegible]tended by operator	VC only relays mode transition command to part of intended actuators: mutually dependant actuators operate in incompatible level of autonomy	
	Causal factors	VC malfunction Wiring malfunction Actuator's malfunction Required level of autonomy is not available for particular actuator		Software architecture allows operator to arbitrarily change actuator's level of autonomy	
	Mitigation measure	Software development and checks Extensive commissioning tests Backup VC Wiring redundancy	Software development and checks	Extensive commissioning tests Software and hardware improvement according to operators' suggestions [illegible]evelopment and checks	

Results

	Significant	Moderate	Minor
Phenomena			
Model			
Assumptions			
Data			
Consensus			

Number	Description	Control action is not provided
A7 Commands	Results in	VC does not relay mode transition command to actuator
	Causal factors	VC malfunction Wiring malfunction Actuator's malfunction Required level of autonomy is not available for particular actuator
	Mitigation measure	Software development and checks  Extensive commissioning tests  Backup VC  Wiring redundancy 

Results


Breakdown of uncertainties by their magnitude
5%
47%
48%
MINOR
MODERATE
SIGNIFICANT
Uncerta
re-oriented
30
20
10
Uncertainties
Model
Assumptions
Data
Consensus
Within shore fa
Within vessel

Results

Advantages

- Promotes search for better-supported safety measures;
- Indicates areas requiring further research;
- Simple to perform.

Drawbacks

- Subjective;
- Inconclusive;
- Only pertains to certain part of safety analysis;
- Does not assess the feasibility of particular safety recommendation;
- Does not reduce potential for uknown unkowns.

Conclusions

The emergence of a completely new technology of an unmanned shipping creates an opportunity to test STAMP applicability to safety-guided design from the very beginning of its development.

However, STAMP is also a relatively new tool and requires certain improvements.

By presenting a method of assessing uncertainties in safety recommendations' elaboration, we hope to make our modest contribution to making STAMP even more thorough.

As for the unmanned ships, the results indicate that their implementation will require embedding safety controls on multiple levels and hierarchy and involving numerous components.

Thank you for your attention

Gdynia Maritime University
ul. Morska 81 – 87
81 – 225 Gdynia

k.wrobel@wn.am.gdynia.pl

www.am.gdynia.pl
facebook.com/Akademia.Morska.w.Gdyni