Basnet, Sunil; Valdez Banda, Osiris; Hirdaris, Spyros

The Management of Risk in Autonomous Marine Ecosystems – Preliminary Ideas

Published in:
Proceedings of the First International Workshop on Autonomous Systems Safety

Published: 01/01/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Basnet, S., Valdez Banda, O., & Hirdaris, S. (2019). The Management of Risk in Autonomous Marine Ecosystems – Preliminary Ideas. In M. A. Ramos, C. Thieme, I. B. Utne, & A. Mosleh (Eds.), Proceedings of the First International Workshop on Autonomous Systems Safety (pp. 112-121). Norwegian University of Science and Technology.

The Management of Risk in Autonomous Marine Ecosystems – Preliminary Ideas

Sunil Basnet(*), Osiris A. Valdez Banda, and Spyros Hirdaris

[1] Marine Technology, Department of Mechanical Engineering, Aalto University, Finland.
(*) sunil.basnet@aalto.fi

Marine industry is set to experience a change of an era as the development of autonomous ships has already started. However, the operation of autonomous ships is not possible unless the new types of hazards and its associated risks due to the rapid technological changes are identified and controlled. Thus, it is necessary to identify or develop a suitable risk management model that can identify these new types of risks.

This paper aims to identify and suggest a suitable risk management model or a category of models for managing the risks in autonomous marine ecosystems. Firstly, the available models and their categories in all major domains such as aviation, automotive, railway and marine industry are explored. Then, a SWOT analysis is conducted for each model category to assess the strengths, weaknesses, opportunities and threats. The results of the SWOT analysis show that the systemic models such as STAMP can be a suitable option than the traditional categories such as sequential and epidemiological models.

Introduction

Because of the continuous development of autonomous technologies, the marine industry currently explores feasible options for the design and operation of maritime autonomous systems [1]. Cross-modal technology disruption trends imply new risks. Hence, it becomes essential to understand gaps in existing risk management systems and explore the potential of novel risk assessment methods especially considering societal and industry expectations for sustainable life cycle solutions [2].

Whereas the marine industry traditionally utilized operational data to understand risks, autonomous marine systems are new and their development is based on limited databases. A direct influence of this is that quantitative risk assessment (QRA) methods and passive risk management practices become less relevant [3]. This is the reason why there is a need to develop new dynamic risk assessment models that are suitable for detecting multiplicity of risks implied by the impact of disruptive technologies, limited human – machine interaction and limited in service experience.

At first instance, the limited availability of data and experience in the maritime domain suggest the opportunity to learn from other industries such as automotive, railway and aviation. As a first step toward this direction, this paper aims to explore the potential of available cross-modal risk management methods and frameworks and then suggest some initial thinking directions in terms of developing techniques and models that may be more suitable for the marine domain.

Methodology

In this paper the available hazard and accident analysis models for risk management used by aviation, railway, automotive and maritime domains are explored and models are then classified based on the taxonomy suggested by Underwood and Waterson [4]. A SWOT analysis is then performed for each category with the aim to understand their potential of implementation. The details of the SWOT analysis and the detailed review of other transport domains are presented in Manzur et al. [5].

Literature Review – Exploring hazard and accident analysis models in major domains

Over the years various systems analysis models and tools have been developed. Figure 1 presents the timeline of the best-known risk management methods [6]. From a critical review perspective, it appears that the railway industry has been leading the way in terms of implementation. For example, highly - automated systems such as the magnetic track inspection systems have been introduced since 1910 with the aim to supplement human inspection [7]. Railway regulatory bodies have recommended the usage of traditional methods such as Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA) and Hazard and Operability study (HAZOP) for managing the risks of modern trains with the higher implementation of automated systems. Recently, Belmonte et al. [8] and Dong [9], suggested the implementation of modern methods such as the Functional Resonance Accident Method (FRAM) and System-Theoretic Accident Model and Processes (STAMP). It is believed that these modern methods may present a good addition to the classical approaches as they cover the complex interactions of modern systems.

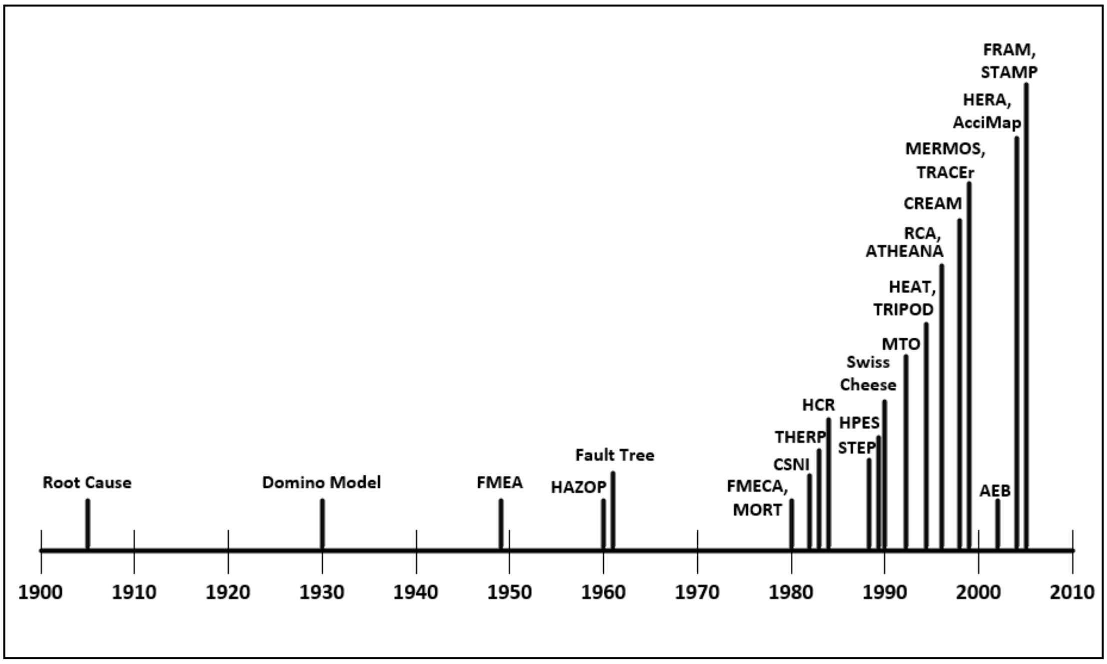


Figure 1. Development of best-known hazard and accident analysis models (adapted from [6]).

Over the past decade, the aviation industry also started using systemic methods. For example, [10–12] suggest that such methods are more effective in terms of assessing system complexity and component interactions. Yet, classic methods are still used primarily because of their long presence.

The automotive industry presents an interesting domain in terms of the potential to link modern risk assessment methods with safety standards. For example, ISO 26262 was developed for ensuring the functional safety of the systems in the automotive domain [13]. However, it does not demand a specific method to be included in the risk management process [14]. Nevertheless, whereas in a similar fashion to aviation industry classic methods are popular, some studies such as [15] and [16] have suggested that a systemic method, STPA, can be a better option as it can be applied to a new system design from an early stage to determine the detailed list of functions, failures and mitigation measures, even without having a detailed information of the design.

In the maritime domain, the Formal Safety Assessment introduced by the International Maritime Organization (IMO) has been widely used for the development and use of risk management practices. The IMO FSA framework [17] does not specify the risk methods to be used. Yet, there is a list of approaches (e.g. FTA, FMEA, HAZOP, HAZID) depending on the types of systems and their stage of design or operational implementation/management. With the rapid development of autonomous systems, the necessity to develop more suitable methods that may handle systemic risks and dysfunctional interactions between system components seems essential.

Categories of Analysis Models

Perrow [18] developed a matrix which classifies different domains based on the manageability and coupling of their systems. Underwood and Waterson [4] has then suggested different categories of analysis models that are suitable for the quadrants in the afore-mentioned Perrow-matrix (see Figure 2). These categories are specified as sequential, epidemiological and systemic. Sequential models consist of methods that have a pre-described path and therefore linear correlation between the origin of an accident (the root cause) and the outcome (the effect). The methods such as Domino model, FTA, FMEA and Root Cause Analysis are classified in this category [4]. Epidemiological methods view accidents as a combination of “latent” and “active” failures within the system. Latent conditions link with working practices (e.g. management and organizational culture) that drive the dynamics between good intentions and actual working procedures. The most popular epidemiological models are Swiss Cheese Model, the Human Factor Analysis & Classification System (HFACS), and the ATSB accident investigation model [4]. Finally, systemic models such as STAMP use the application of systems theory and describe accidents as the result of lack of safety constraints to control the scenarios generated due to unsafe component interactions in a system [19].

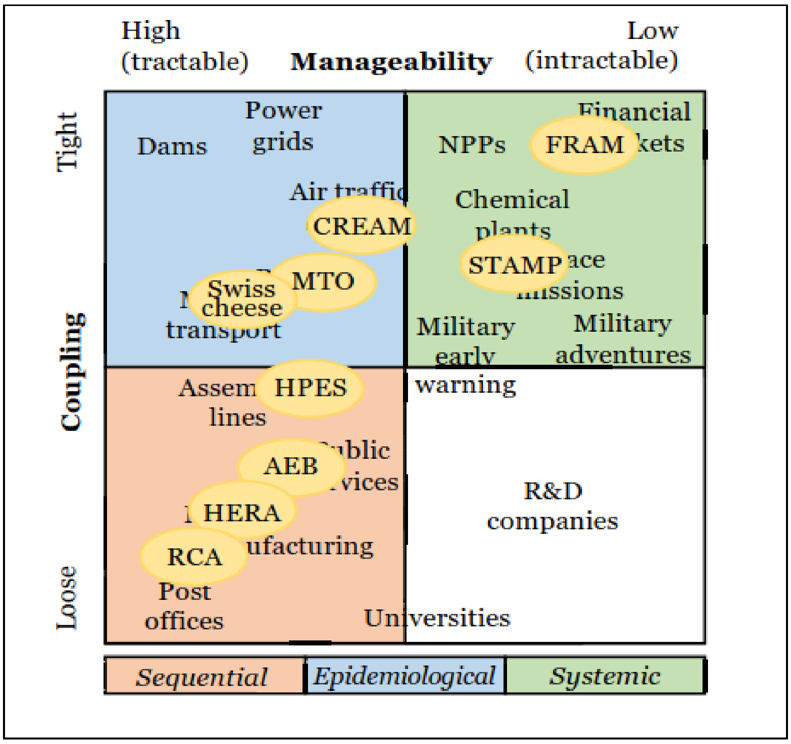
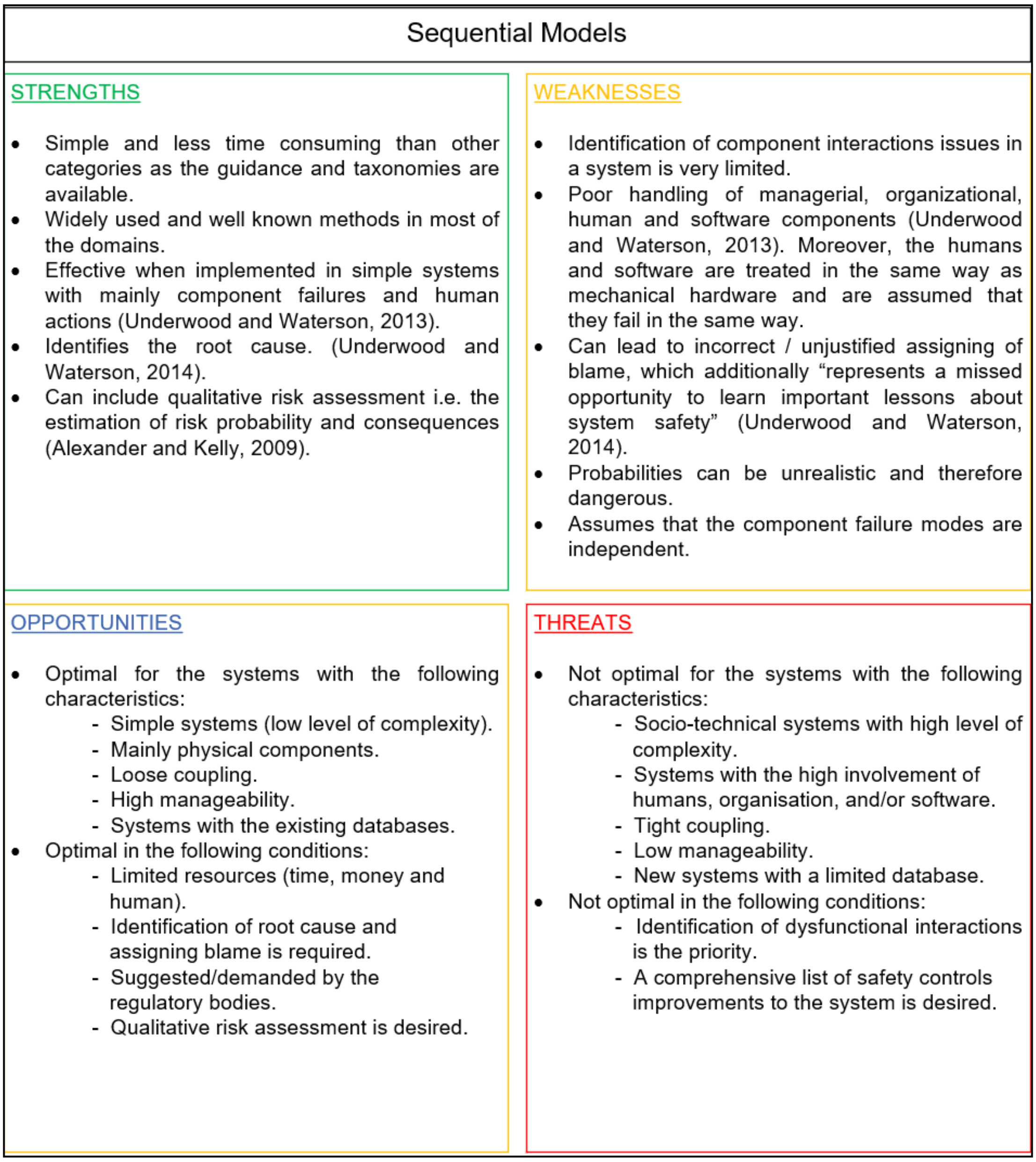


Figure 2. Hazard and accident analysis models categories suitable for different sets of domains in Perrow-matrix (adapted from [4]).

Swot Analysis

A SWOT analysis was then conducted for analyzing the strengths, weaknesses, opportunities and threats of each of the analysis models categories. The SWOT analysis of sequential models, epidemiological models and systemic models are presented in Figure 3, Figure 4 and Figure 5 respectively.



Sequential Models

STRENGTHS

- Simple and less time consuming than other categories as the guidance and taxonomies are available.
- Widely used and well known methods in most of the domains.
- Effective when implemented in simple systems with mainly component failures and human actions (Underwood and Waterson, 2013).
- Identifies the root cause. (Underwood and Waterson, 2014).
- Can include qualitative risk assessment i.e. the estimation of risk probability and consequences (Alexander and Kelly, 2009).

WEAKNESSES

- Identification of component interactions issues in a system is very limited.
- Poor handling of managerial, organizational, human and software components (Underwood and Waterson, 2013). Moreover, the humans and software are treated in the same way as mechanical hardware and are assumed that they fail in the same way.
- Can lead to incorrect / unjustified assigning of blame, which additionally "represents a missed opportunity to learn important lessons about system safety" (Underwood and Waterson, 2014).
- Probabilities can be unrealistic and therefore dangerous.
- Assumes that the component failure modes are independent.

OPPORTUNITIES

- Optimal for the systems with the following characteristics:
    - Simple systems (low level of complexity).
    - Mainly physical components.
    - Loose coupling.
    - High manageability.
    - Systems with the existing databases.
- Optimal in the following conditions:
    - Limited resources (time, money and human).
    - Identification of root cause and assigning blame is required.
    - Suggested/demanded by the regulatory bodies.
    - Qualitative risk assessment is desired.

THREATS

- Not optimal for the systems with the following characteristics:
    - Socio-technical systems with high level of complexity.
    - Systems with the high involvement of humans, organisation, and/or software.
    - Tight coupling.
    - Low manageability.
    - New systems with a limited database.
- Not optimal in the following conditions:
    - Identification of dysfunctional interactions is the priority.
    - A comprehensive list of safety controls improvements to the system is desired.

Figure 3. A SWOT analysis of the sequential models.

Epidemiological Models

STRENGTHS

- Simple and less time consuming than systemic models.
- Some advanced methods in certain situations can provide similar results as the systemic models with less drawback (Underwood and Waterson, 2014)
- Less resource intensive than systemic methods.
- In addition to the identification of active failures (similar to sequential methods), it also identifies latent / organisational factors.
- Widely used in several domains. (Underwood and Waterson, 2014)

WEAKNESSES

- Cannot provide the same depth of results as systemic methods since the dynamic factors and non-linear interactions between components are not considered. (Yousefi et al., 2018)
- Focusing on the identification of root cause can lead to the incorrect / unjustified assigning of blame.

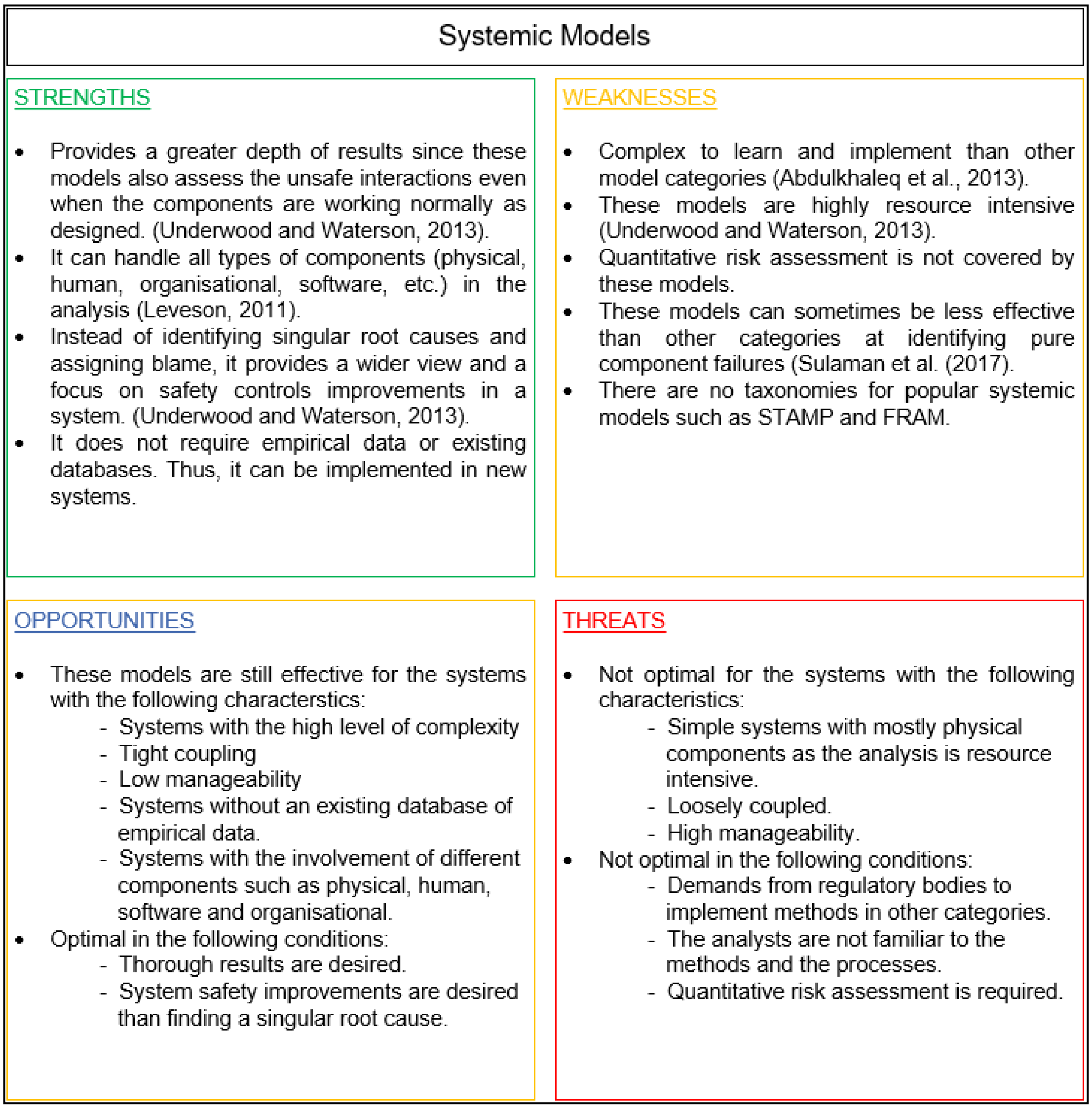
OPPORTUNITIES

- Optimal for the systems with the following characteristics:
  - Involvement of physical, human and organisational factors.
  - Few software components
  - Tight coupling
  - High manageability
  - Systems with the existing databases.
- Optimal in the following conditions:
  - Limited resources (time, money and human)
  - Identification of root cause and assigning blame is required.
  - Suggested/demanded by the regulatory bodies.

THREATS

- Not optimal for the systems with the following characteristics:
  - Socio-technical systems with high level of complexity.
  - Systems with high software implementation.
  - Low manageability
  - New systems with a limited database.
- Not optimal in the following conditions:
  - Identification of dysfunctional interactions is the priority.
  - A comprehensive list of safety improvements to the system is desired.

Figure 4. A SWOT analysis of the epidemiological models.



Systemic Models

STRENGTHS

- Provides a greater depth of results since these models also assess the unsafe interactions even when the components are working normally as designed. (Underwood and Waterson, 2013).
- It can handle all types of components (physical, human, organisational, software, etc.) in the analysis (Leveson, 2011).
- Instead of identifying singular root causes and assigning blame, it provides a wider view and a focus on safety controls improvements in a system. (Underwood and Waterson, 2013).
- It does not require empirical data or existing databases. Thus, it can be implemented in new systems.

WEAKNESSES

- Complex to learn and implement than other model categories (Abdulkhaleq et al., 2013).
- These models are highly resource intensive (Underwood and Waterson, 2013).
- Quantitative risk assessment is not covered by these models.
- These models can sometimes be less effective than other categories at identifying pure component failures (Sulaman et al. (2017).
- There are no taxonomies for popular systemic models such as STAMP and FRAM.

OPPORTUNITIES

- These models are still effective for the systems with the following charactersitics:
  - Systems with the high level of complexity
  - Tight coupling
  - Low manageability
  - Systems without an existing database of empirical data.
  - Systems with the involvement of different components such as physical, human, software and organisational.
- Optimal in the following conditions:
  - Thorough results are desired.
  - System safety improvements are desired than finding a singular root cause.

THREATS

- Not optimal for the systems with the following characteristics:
  - Simple systems with mostly physical components as the analysis is resource intensive.
  - Loosely coupled.
  - High manageability.
- Not optimal in the following conditions:
  - Demands from regulatory bodies to implement methods in other categories.
  - The analysts are not familiar to the methods and the processes.
  - Quantitative risk assessment is required.

Figure 5. A SWOT analysis of the systemic models.

Discussion

The literature review and the SWOT analysis presented in this paper imply that understanding complex interactions between technologically disruptive systems is an important first step in terms of estimating their potential implementation within the context of managing autonomy related risks and defining risk management systems of relevance based on risk control options. Across multi-modal domains, it becomes obvious that autonomous systems and operations are defined by components and subsystems that are interconnected. In this sense, manageability becomes critical in terms of understanding risks associated with system functionality. Another key point to consider is intractability especially for cases where principles of functioning are unknown, while a high level of detail is essential to understand the dynamic interactions of sub-systems. Accordingly, the high complexity and interconnectivity of autonomous systems are key factors and should be considered in terms of defining unified approaches and risk management models in autonomous marine domain.

The comparison of the strengths, weaknesses, opportunities and threats of all categories shows that the systemic models are the most suitable models for the systems with tight coupling and low manageability. Furthermore, these models are also effective in systems with the high involvement of different components such as physical, human, organizational and software. Moreover, the systemic models do not require empirical data as these models do not aim to estimate the probability of risk occurrence and consequences. In addition, these models have several other benefits such as providing a wider view and focus on safety control improvements and an assessment of dysfunctional interactions even in normally operating components. As all these features are required in autonomous marine ecosystems, this study shows that the systemic models can be a suitable option to analyses the autonomous systems in marine industry and manage risks from the earliest design phase.

Conclusions

The review presented in this paper suggests that modern risk assessment practices (e.g. FRAM, STAMP) could be a foundation or an optimal choice for the risk assessment of autonomous marine systems especially considering the sub- system complexity and interconnectivity of autonomous ships and their components. Nevertheless, there are also some drawbacks of using such approaches as they require high resources and well-developed educational practices. Considering that the information on autonomous designs and their functionality is still limited, there is a need to re-consider all available methods in a greater detail. Various factors such as (a) the desired level of thoroughness in comparison to resource consumption; (b) the level of detail in the analysis and (c) the format ad content (risk nodes) that may be demanded by each of the categories for the analysis could be considered to justify any future choices.

References

[1] MUNIN. Research in maritime autonomous systems project results and technology potentials. 2016.

[2] Thieme CA, Utne IB, Haugen S. Assessing ship risk model applicability to Marine Autonomous Surface Ships. Ocean Eng 2018;165:140–54. doi:10.1016/j.oceaneng.2018.07.040.

[3] Montewka J, Wróbel K, Heikkilä E, Valdez Banda OA, Goerlandt F, Haugen S.

Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping. PSAM 14th Probabilistic Saf Assess Manag Conf 2018.

[4] Underwood PJ, Waterson PE. Accident analysis models and methods: guidance for safety professionals. 2013.

[5] Manzur Tirado AM, Brown R, Valdez Banda OA. Risk and Safety management of autonomous systems: a literature review and initial proposals for the maritime industry [online]. 2019.

[6] Hollnagel E. From FRAM (Functional Resonance Accident Model) to FRAM (Functional Resonance Analysis Method) 2008.

[7] Garrett M, Boslaugh SE. Railroad Automation Technology. Encycl. Transp. Soc. Sci. Policy, 2014. doi:10.4135/9781483346526.n396.

[8] Belmonte F, Schön W, Heurley L, Capel R. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway trafficsupervision. Reliab Eng Syst Saf 2011. doi:10.1016/j.ress.2010.09.006.

[9] Dong A, Leveson N. Application of Cast and Stpa To Railroad Safety in China. Massachusetts Inst Technol 2012.

[10] Ishimatsu T, Leveson N, Thomas J, Katahira M, Miyamoto Y, Nakao H. Modeling and hazard analysis using STPA. Eur. Sp. Agency, (Special Publ. ESA SP, 2010.

[11] Allison CK, Revell KM, Sears R, Stanton NA. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. Saf Sci 2017. doi:10.1016/j.ssci.2017.06.011.

[12] Fleming CH, Spencer M, Thomas J, Leveson N, Wilkinson C. Safety assurance in NextGen and complex transportation systems. Saf Sci 2013. doi:10.1016/j.ssci.2012.12.005.

[13] Czerny BJ, Ambrosio JD, Debouk R. ISO 26262 Functional Safety Draft Intrenational Standard for Road Vehicles: Background, Status and Overview. 2011.

[14] Abdulkhaleq A. Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain Motivation : STAMP / STPA Application Areas 2013:1–17.

[15] Abdulkhaleq A, Wagner S, Lammering D, Boehmert H, Blueher P. Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles 2017:11–24.

[16] Sabaliauskaite G, Liew LS, Cui J. Integrating Autonomous Vehicle Safety and Security Analysis Using STPA Method and the Six-Step Model. Int J Adv Secur 2018.

[17] International Maritime Organization (IMO). https://edocs.imo.org/Final Documents/English/MSC-MEPC.2-Circ.12-Rev.1 (E).docx. vol. 44. London: 2015.

[18] Perrow C. Normal accidents: Living with high risk technologies. 1999. doi:10.5465/AMR.1985.4278477.

[19] Leveson N. Engineering a safer world: systems thinking applied to safety. The MIT Press; 2016. doi:10.5860/choice.49-6305.