
This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Valdez Banda, Osiris A.; Goerlandt, Floris

A STAMP-based approach for designing maritime safety management systems

Published in:
Safety Science

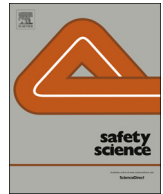
DOI:
[10.1016/j.ssci.2018.05.003](https://doi.org/10.1016/j.ssci.2018.05.003)

Published: 01/11/2018

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

Published under the following license:
CC BY-NC

Please cite the original version:
Valdez Banda, O. A., & Goerlandt, F. (2018). A STAMP-based approach for designing maritime safety management systems. *Safety Science*, 109, 109-129. <https://doi.org/10.1016/j.ssci.2018.05.003>



A STAMP-based approach for designing maritime safety management systems

Osiris A. Valdez Banda^{a,*}, Floris Goerlandt^{a,b}

^a Aalto University, Department of Mechanical Engineering (Marine Technology), Research Group on Maritime Risk and Safety, Espoo, Finland

^b Dalhousie University, Department of Industrial Engineering, Halifax, Nova Scotia B3H 4R2, Canada

ARTICLE INFO

Keywords:

System safety engineering
Safety management systems
STAMP
Maritime safety
Vessel traffic services
Key performance indicators
Safety performance monitoring tool

ABSTRACT

Designing maritime safety management systems commonly follows basic processes which focus on fulfilling the demands of the regulations in the industry. This provokes designing systems with limited application which are not capable to efficiently use the guidance contained in regulatory demands, and more importantly, creating systems which are not capable of representing, evaluating, and improving the dynamic management of safety-critical organizations. This article proposes a safety system engineering process for designing maritime safety management systems which is based on the Systems-Theoretic Accident Modelling and Processes (STAMP). This process is applied for sketching the safety management of the Vessel Traffic Services in Finland. The aim is to systematically represent the function of the utilized controls for ensuring the internal VTS safety management and the safety of navigation in Finnish sea areas. The outcome of this study provides a descriptive process of analysis for designing maritime safety management systems. In this process, two other concrete elements are included for supporting the functioning of the safety management system to be designed. First, the adaptation of an identification process for determining key performance indicators for planning, monitoring and evaluating the functioning of the safety management system. Second, the constitution of a performance monitoring tool capable of executing the monitoring, measuring, and updating of the determined key performance indicators and the general functioning of the designed safety management system.

1. Introduction

Maritime navigational operations are commonly categorized as one of the most complex and dangerous industry within the large industrial sectors globally (Celik, 2009; Hetherington et al., 2006). For this reason, the International Maritime Organization (IMO) continuously attempts to ensure the safety of maritime operations by providing international conventions such as the International Convention for the Safety of Life at Sea (SOLAS) and particular safety management guidelines such as the International Management Code for the Safe Operation of Ships and Pollution prevention (ISM Code). These and other regulations have brought a gradual improvement of the safety of maritime operations and maritime organizations in general (Kristiansen, 2013). However, the effect of these safety regulations and guidelines on having an actual proactive approach to maritime safety is still being questioned (Schröder-Hinrichs et al., 2013). Hitherto, in

certain sectors of the maritime industry, the design and implementation of their safety management systems (SMS) are still influenced by a common limited approach which focuses on fulfilling the demands of the regulations applicable to the organization (Schröder-Hinrichs, 2010).

This issue can be extended with the identified lack of processes for designing and implementing safety management systems capable of representing and constantly improving the management of safety-critical organizations (Dekker, 2014; Hollnagel, 2014; Leveson, 2011; Oltedal and Wadsworth, 2010; Reason, 1998; Reiman and Oedewald, 2007). Studies done for the establishment of a framework to design safety management systems in the nuclear power industry represent few of the available examples for this purpose (Falk et al., 2012; Wahlström and Rollenhagen, 2014). Another issue is the common disregard of the guidance already available in safety regulations and guidelines which can efficiently support the actual organizational safety

Abbreviations: BN(s), Bayesian Network(s); CMO, Context-Mechanism-Outcome; EA, Environmental Assumption; IALA, International Association of Lighthouse Authorities; IMO, International Maritime Organization; ISM Code, International Management Code for the Safe Operation of Ships and Pollution Prevention; KPI(s), Key performance Indicator(s); PDCA, Plan-Do-Check-Act; Req., Requirement of the SMS; SC, Safety Constraint; SMS, Safety Management System(s); SOLAS, International Convention of Safety of Life at Sea; STAMP, Systems-Theoretic Accident Model and Processes; STPA, Systems-Theoretic Process Analysis; UCA, Unsafe Controlled Action; VTS, Vessel Traffic Services

* Corresponding author.

E-mail address: osiris.valdez.banda@aalto.fi (O.A. Valdez Banda).

management and therefore demonstrate their fulfilment (Reese, 2015; Valdez Banda et al., 2016b).

In the context of maritime navigational operations, the need for SMS capable of representing and actually supporting the development of the operations have also been detected in (Boström and Österman, 2016; Ek and Akselsson, 2005; Flin et al., 2000; Hänninen et al., 2014; Lappalainen et al., 2014; Oltedal, 2009; Reason, 2005). A clear example is presented in Valdez Banda et al., (2016a). The analysis of determined actions to reduce the risk of winter navigation operations has pointed out that, in practice, there is lack to translate the actual operational needs into the functioning of the organizational SMS.

In this study, a STAMP-based approach for designing maritime safety management systems is presented. The proposed process is guided by the application of a methodology for integrating safety into system engineering which is based on the design of the organizational safety intent specification included in the Systems-Theoretic Accident Modelling and Processes (STAMP) presented in Leveson (2011).

A case study for the application of the process is presented in the analysis of the safety function in Vessel Traffic Services (VTS) in Finland. VTS is one of the main actors responsible for monitoring and controlling the safety and smooth development of maritime traffic (Praetorius et al., 2015). Thus, the objective is to systematically represent the functioning of VTS Finland and the controls utilized to ensure their internal safety management and the safety of the navigation in Finnish sea areas. The analysis covers the functioning of aid services provided by VTS all year around, making distinctions between services provided during spring-summer-autumn season and winter ice season.

The application of the proposed process culminates with a defined SMS for VTS Finland and the provision of a performance monitoring tool that implements a set of identified Key Performance Indicators (KPIs) which are created to support the planning, monitoring, evaluating and updating of the requirements of the designed SMS for VTS Finland.

2. Safety management perspective

The general notion of safety management has been discussed and various concepts have been developed and applied in different industrial sectors. In the context of safety-critical organizations, the actual management of safety must understand the nature of the aspects influencing how an organization ensures the safety of the operations (Reason, 1997). For this, the top management commitment, the proactive involvement of all personnel in the organization, and the provision of skills, appropriate guidance and tools are essential to obtain the safety management targets (Grote, 2012; Leveson, 2011). The combination of these elements is essential to execute the required tasks to achieve the organizational safety goals and simultaneously fulfil the demands of regulations (Hollnagel, 2014).

A SMS is the commonly utilized vehicle to achieve the safety objectives of an organization. Therefore, SMS must effectively understand the nature of the internal functioning of the organization while also effectively implement and comply the applicable safety regulations. This creates evidence that safety, in general, is a system property, and therefore it must be managed at the system level (Leveson, 2011). Thus, the main objective of any SMS is to prevent accidents, therefore SMS has to be able to understand, monitor and improve the safety performance of the organization (Dekker, 2014).

Commonly, the performance of SMS is monitored and measured by implementing KPIs (Reiman and Pietikäinen, 2012). These measure the current levels of operational and organizational safety represented in the performance of the SMS. At the same time, KPIs should capture and represent organizational safety trends and developments (Øien, 2001). Moreover, the use of KPIs increases the knowledge gathered in the SMS and proactively improve the management of safety (Swuste et al., 2016). Fig. 1 presents the foundation behind the elements interacting in

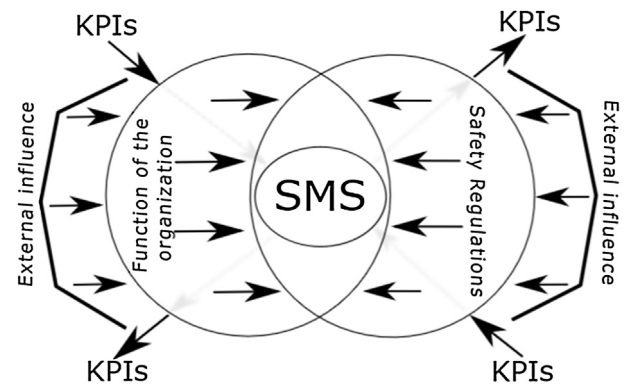


Fig. 1. Elements influencing and interacting in the function of SMS.

the dynamics of any SMS. First, the actual functioning of the organization, the internal managerial and operational practices. Second, the demands included in the safety regulations applied to the organization. Third, the external influence affecting the two previous elements, the influence from the acting of customers, industry, economy, society, and regulatory organizations. These three elements influence the actual performance of the SMS. Finally, the SMS performance is commonly measured and guided with the use of KPIs.

3. Research methodology

Fig. 2 presents a flowchart describing the steps of the research methodology. First, the description of the study methodology foundations. This includes the STAMP methodology and the STAMP safety intent specification. Second, the methodology for establishing the process for designing maritime safety management systems. It includes the design process and the method to define the KPIs of the SMS. Third, the methodology of the monitoring tool. The practicalities of the tool to implement the KPIs and monitor the performance of the SMS.

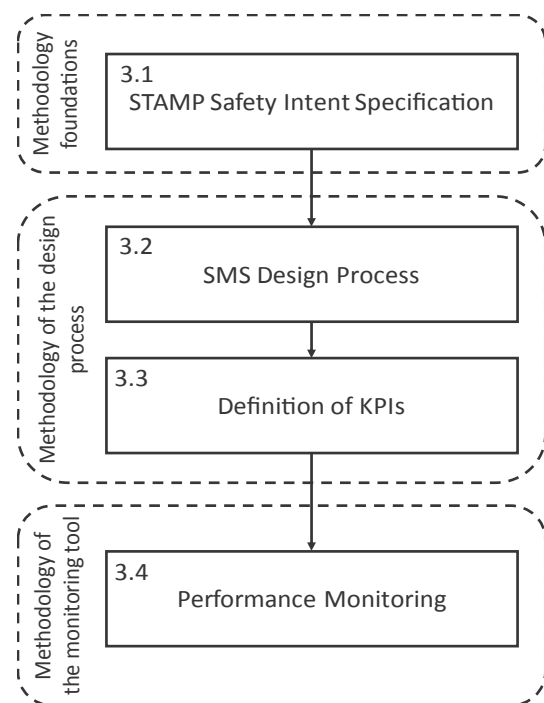


Fig. 2. Description of the methodology applied in the study. At each component in the figure, the reference to a section which describes the utilized method is provided.

	Environment	Operator	System and components	Verification and validation
Level 0: Program management	Management plans, safety plan, safety management procedures and safety plans			
Level 1: System purpose	Assumptions and constraints	Responsibilities Requirements	Goals, requirements, design, constraints and limitations	Preliminary Hazard analysis
Level 2: System principles	External interfaces	Task analysis and allocation, Controls and Displays	Logic principles, functional decomposition and allocation	Validation plan and System Hazard analysis
Level 3: System architecture	Environment models	Operator Task models and HCI models	Blackbox functional models and Interface specifications	Analysis plans and results, Subsystem Hazard analysis
Level 4: Design representation		Human – Computer Interface Design	Software and hardware design aspects	Test plans and results
Level 5: Physical representation		Guided User Interface design, physical control design	Software code, hardware assembly instructions	Test plans and results
Level 6: System operations	Audit procedures	Operator manuals, Maintenance and training materials	Error reports, and change request.	Performance monitoring (KPIs)

Fig. 3. The structure of the safety intent specification (adapted from Leveson (2011)).

3.1. Systems-theoretic accident modelling and processes (STAMP)

3.1.1. Foundations

STAMP is an approach to depict and review the function of safety from a systemic perspective. It assesses the function of safety in complex socio-technical systems. It attempts to efficiently face the fast pace of technological change, increase the ability to learn from experience, understand the changing nature of accidents, and particularly deal with the complexity from the interaction among diverse system components (Leveson, 2011). Previously, STAMP has been applied in the analysis of safety in the aircraft industry (Chatzimichailidou and Dokas, 2015; Fleming et al., 2013; Passenier et al., 2015; Stringfellow et al., 2010) and recently for the analysis of risks in automated automotive systems (Thomas and Suo, 2015). In the maritime domain, STAMP has been applied for the analysis of safety adaptive management of the maritime spatial planning at the Gulf of Finland (Aps et al., 2015, 2016) and the analysis of the Sewol Ferry accident in South Korea (Kim et al., 2016; Lee et al., 2017).

The foundations of the STAMP question the theoretical background of traditional safety approaches which treat safety as a reliability problem, thus following the common idea that if system components do not fail accidents won't occur. For this, STAMP assesses that accidents are actually complex processes which involve the entire socio-technical system. Furthermore, STAMP questions traditional approaches which assume most of the accidents are caused by operator's error when actually operator's behaviour and performance are product of the environment in which it occurs. The method presents several integrated aims to the foundation of organizational safety:

- Providing a more systemic way to model accidents and safety for producing a better and less subjective understanding about how accidents occur and how they can be prevented.
- Allowing and encouraging new types of hazard analysis and risk assessment which go beyond component failures.
- Shifting from human errors to focus on mechanisms that shape human behaviour.
- Encouraging a shift in the emphasis in accident analysis from “cause” to “understanding”.
- Encouraging multiple safety view points and interpretations.
- Assisting in the definition of operational metrics and analysis of

performance data.

The foundations of STAMP rest on the emergence and hierarchy and communication (feedback) and control. Emergence is the representation or model of complex systems, hierarchy describes different levels of an organization and each level has emergent properties. Communication (feedback) transmits the understanding about the hierarchy and its emergent properties for imposing control constraints on system behaviour to avoid unsafe events. In this study, special attention is given to the creation of the hierarchical control structure of maritime organizations. The aim is to analyse potential organizational control processes that describe the safety constraints at the different levels in the organizations hierarchy.

Organizational control process involves determining what work is needed to accomplish the goal, assigning tasks to individuals, and arranging those individuals in a decision-making framework (Mayes and Allen, 1977). A safety constraint is any constraint that specifies a determined safety controller (e.g. architectural safety mechanism, safety design feature, safety implementation technique, or safety process) (Firesmith, 2004). Accidents occur when safety constraints are violated. Moreover, if inadequate controls are set, the constraints may cause inappropriate communication and process feedback (Conant and Ashby, 1970; Sarter and Woods, 1995; Kazaras et al., 2012; Salmon et al., 2012). Therefore, the process for designing the safety intent specification integrated into STAMP (presented in next section) is utilized to design a safety control structure that depicts the safety management of maritime organizations and simultaneously keeps its continued effectiveness as changes and adaptations occur over time.

3.1.2. The safety intent specification in STAMP

Intent specifications are based on systems theory, system engineering principles and psychological research on human problem solving (Leveson, 2011). An intent specification assists humans in dealing with complexity. It differs from the specification based on standard regulations in its structure but not in its content, the main difference is that intent specifications contain more detailed information.

In STAMP, the intent specification is organized into different hierarchy levels which provide information about the reasons behind the design decisions for assembling the management of organizational

safety. Moreover, it describes how these reasons interact in the dynamics of organizational safety management. Fig. 3 presents the structure and the information contained at each level of the intent specification. These levels are classified by their influence on the main elements of the dynamic context of organizational safety management.

Level 0 provides the management view and the relationship between plans and project development status through links to the other parts of the intent specification. Level 1 represents the view of system engineers and customers for building and the intent specification, including the revision of its efficiency. Level 2 provides the system-level design principles. Level 3 specifies the system architecture and it serves as an interface between system engineers and component engineers. Level 4 and 5 provide information to reason about individual components and implementation issues. Level 6 gives a view of the operational system and acts as the interface between development and operations.

3.2. Designing SMS with the safety intent specification

The elements included in the levels of the STAMP safety specification are the basis to elaborate the process for designing maritime SMS. Each level provides guidance for designing the system and for establishing and maintaining the elements defined during the design phase. Fig. 4 presents a guided process for designing SMS. This process is practically implemented and the outcome is presented in Section 4.2.

Level 0 provides the initial definition of the connection between the planning of goals and the existing management practices in the organization. This is done with the review of the organizational management systems implemented in the organization (task 0.1). It includes reviewing standardized work procedures and directions for regulatory compliance. This promotes integration and efficient connectivity between the organizational management systems.

Level 1 is the most elaborated in designing the maritime SMS. This defines the foundations of the SMS which represent the safety components to be analysed and included in the initial structure of the SMS. These are based on the combined view of system external and internal

customers and engineers. This level represents the basis for determining the design rationale with clear and detailed safety considerations of the system. At this level, the general system requirements and control constraints are determined. In order to achieve this, the following tasks are executed:

- Identify and defined accidents (1.1). Accidents represent undesired and unplanned events that result in loss and affectations, including loss of human life or injury, property damage, equipment damage, environmental pollution, delays, and repair costs.
- Hazard identification (1.2). It enables the analysis of the actual triggers of the listed accidents. This process is a common brainstorming for defining the potential causes of accidents. The aim is to promote participation and collect relevant information.
- Preliminary hazard analysis (1.3). In this type analyses, risk is defined as a combination of severity and likelihood (Leveson, 2011). Severity provides the level of affectation to the most relevant elements that the system is aiming to ensure. The likelihood is the evaluation of the hazard occurrence. The analysis incorporates evaluates accident data and the knowledge of the functioning of the elements affected by the hazards.
- Document environmental assumptions (1.4). These represent the specifications of the system requirements and the features of the hazard analysis. These ensure the system operation and maintenance as planned in the design phase. These provide the understanding of the operational context of the system. The documenting of assumptions avoid safety violations caused by posterior changes in the system.
- Initial restrictions of the SMS (1.5). Any system has limited scope, therefore specifying the functional restrictions of the system in the design phase is important. This facilitates the understanding of the system function and enables a more accurate delegation of the system's responsibilities.
- Requirements of the SMS (1.6). This task defines the goals of the SMS into testable and achievable high-level requirements. These

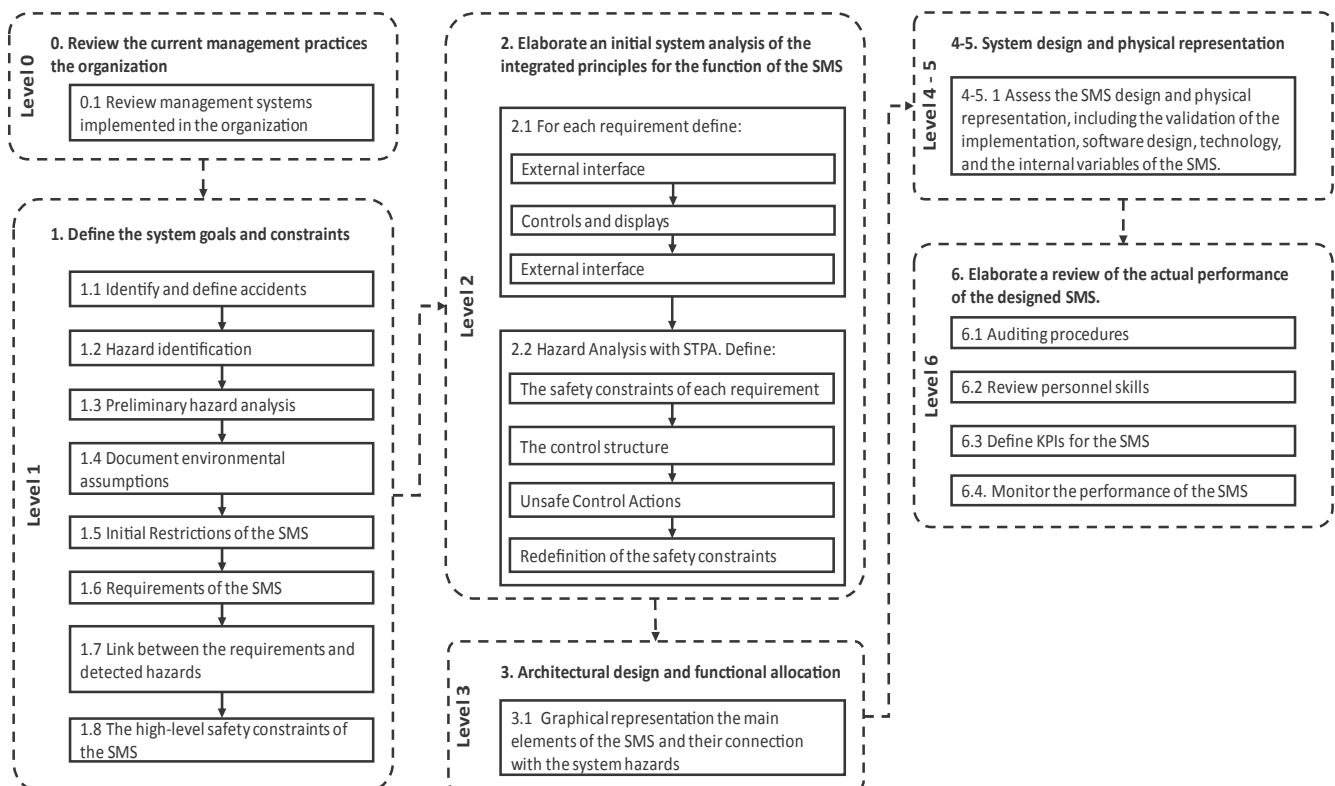


Fig. 4. Process for designing SMS with the STAMP safety intent specification.

requirements include the formal assumptions which determine more concrete targets in the functioning of the system.

- The link between the requirements and detected hazard (1.7). The link provides traceability from requirements to actual implementation. This supports the review of activities and the design of rationale information into the SMS. Thus, when this information has to be updated, this process can be executed by following the link.
- The high-level safety constraints of the SMS (1.8). These are restrictions on the way the system can achieve its purpose. The evaluation and clarification of the trade-offs among alternative designs are essential for this task. Safety constraints represent the executed controls to ensure the mitigation of the identified hazards.

Level 2 extends the details of the design and the scientific and engineering principles of the system. This level enables a first representation of the practical function of the SMS. It presents the safety management as done, identifies the links between the requirements and constraints, and it introduces the actual interfaces, controls, displays, and the logic principle behind the practical application of the requirements (task 2.1). Moreover, it reviews and redefines the requirements and constraints established in level 1. For this, the System-Theoretic Process Analysis (STPA) is implemented (task 2.2.). The STPA is a hazard analysis technique that identifies accident scenarios that encompass the entire accident process by including design errors, component interactions, and other social, organizational, and management factors in the analysis (Leveson, 2011). The STPA consists of two steps:

- Step 1: Identify the potential for inadequate controls of the system that could lead to a hazardous state
- Step 2: Determine how each potentially hazardous control action identified in step 1 could occur

Levels 3 enables a general representation of the elements integrated at levels 1 and 2. The aim is to support the representation of the main elements (SMS requirements and safety constraints) and their connection with the system hazards. This representation should be displayed in a simple manner. For this, a graphical representation the main elements of the SMS and their connection with the system hazards needs to be developed (task 3.1). It should provide a simple form to visualize, communicate and discuss the structure of the SMS.

Levels 4–5 complement the representation of the general function of the SMS, including the engineering principles, technology and equipment which take part in the practical implementation of the system. The purpose is to review, test, and validate the physical implementation, software design, and internal variables of the elements established in the levels 0 to 3. These are required to communicate the system safety demands to the system developers, service and technology providers, and the users of the system. For this, processes need to be established for reviewing how the needs of the system implementers and designers are communicated to the component designers (task 4-5.1).

Level 6 represents the operational part of the system, providing the link between the system development and operations. This level is used to plan the review of the performance of the system. It demands the design of the actions for keeping the system in its optimal function and making it truly proactive. Four tasks are included at this level:

- Auditing procedures (6.1). These analyse the performance of safety management procedures and the SMS in general.
- Review of the personnel skills (6.2). This is done with a Strength-Weaknesses-Opportunities-Threat (SWOT) analysis.
- Define KPIs (6.3). The task is described in Section 3.3.
- Monitor the performance of the SMS (6.4). The task is described in Section 3.4.

3.3. Key performance indicators (KPIs)

Monitoring, reviewing and updating the SMS are essential to keep the system functional and prevent degradation over time (Øien, 2001). This section focuses on defining KPIs for measuring the performance of the SMS (task 6.3). For this task, the method proposed in Valdez Banda et al. (2016b) is utilized. This method performs a systematic evaluation of the safety management practices implemented in the organization. It focuses on the analysis of the requirements demanded in safety management regulations. It enables the integration between the safety regulatory requirements and the actual safety management practices in the organization.

This method is based on “realist evaluation” proposed by Pawson and Tilley (1997). This evaluation originally aims to realistically and constantly assess how the programmes are supposed to function and how efficient their functioning is. For this, the realist evaluation implements the Context-Mechanism-Outcome (CMO) analyses:

- Context assesses and describes the conditions in which the programmes are introduced and applied.
- Mechanisms correspond to the resources and practical applications that make the programmes work.
- Outcome represents the analysis of both intended and unintended consequences derived from the programme implementation.

In the adaptation to the method proposed in Valdez Banda et al. (2016b), the CMO analyses safety management requirements. Thus, the CMO is implemented as follow:

- Context assesses the way the requirements are subjected to the reasoning and environment of the affected organisation.
- Mechanisms review the practical arrangements executed for developing all aspects planned in an SMS. This considers the way the organisation uses the resources to make the system functional and supportive to obtain the planned objectives.
- Outcome executes predefined estimations of all possible consequences arising from the application of these requirements, and how the requirements need to be adapted to the plans, procedures and work processes within an SMS.

The use of this method supports the definition of KPIs with diverse functions for the analysis and management of safety. The literature commonly divides KPIs into so-called leading and lagging indicators. Leading KPIs refer to measures for continuously monitoring identified inputs, which are needed to achieve a planned safety target and/or objective (Reiman and Pietikäinen, 2012). Lagging KPIs are measurements that perform reactive monitoring to identify e.g. when a planned objective or target has not been reached (Øien, 2001). In this study, KPIs are categorized into three groups based on Reiman and Pietikäinen (2012):

- Drive indicators. The definition and monitoring of these KPIs focus on implementing and reviewing certain actions used to change, maintain and reinforce different elements of the system. Their main function is to guide the socio-technical aspect of the system by motivating certain safety-related activities.
- Monitor indicators. These are used for monitoring the function of the system, including but not limited to the efficacy of the safety management practices in the organization. Monitor indicators reflect the capacity of the organization to perform safely.
- Outcome indicators. These reflect a temporary end result of a process and/or an activity in the SMS. An outcome is always the result or consequence of some other factor or combination of factors and circumstances. These indicators focus on the result or consequence of the tasks or processes in the organization.

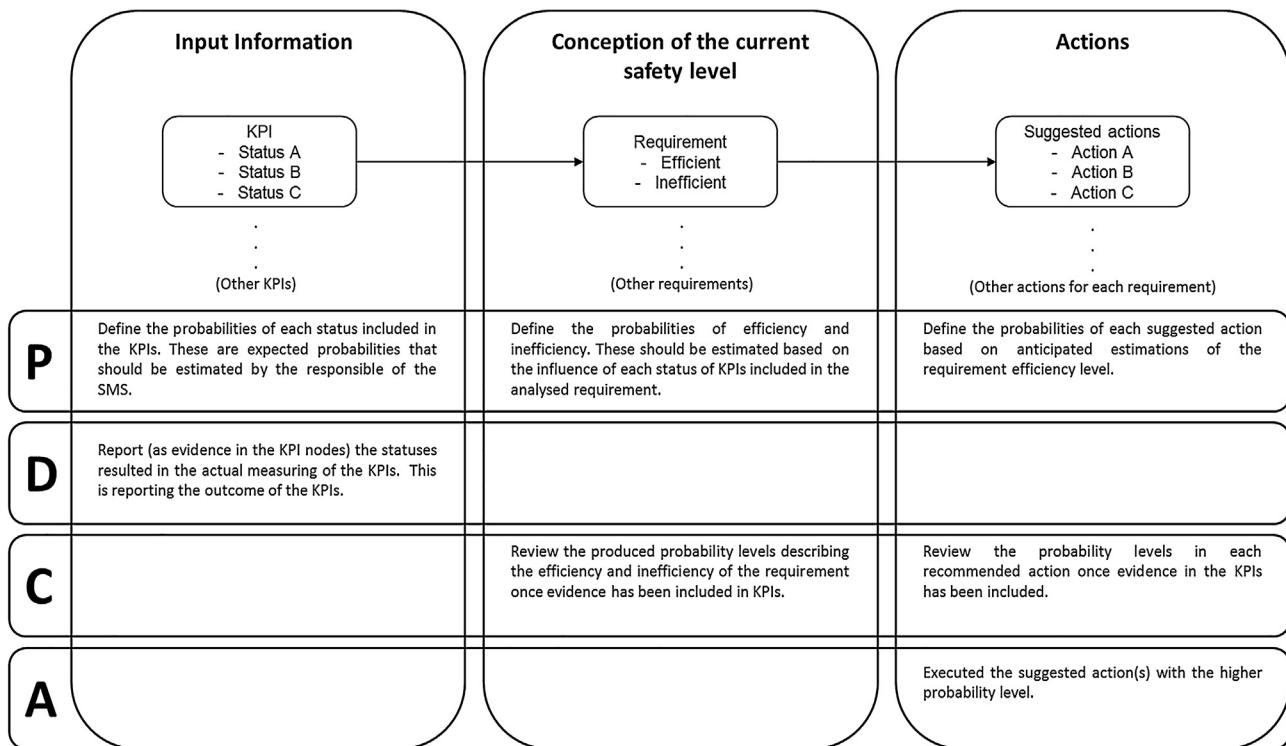


Fig. 5. Functioning of the performance monitoring tool based on the PDCA process.

3.4. The safety performance monitoring tool

Once the KPIs of the SMS are defined, a tool for reporting, monitoring and assessing the KPIs and the performance of the requirements of the SMS is elaborated. For this, Bayesian Networks (BNs) is the modelling technique utilized for the actual monitoring and assessing of KPIs. This technique is selected because BNs can depict relatively complex dependencies and cope with uncertainty while also having a graphical dimension (Pearl, 2014). The aim of this tool is to analyse the performance of the requirements of the SMS through the reporting and measuring of the defined KPIs. The functioning of the tool is structured based on a traditional Plan-Do-Check-Act (PDCA) process. Fig. 5 presents the description of the steps in the PDCA process for establishing and making the tool functionally active. The performance monitoring tool (the main BN model) is divided into three sub models:

1. (Input Information) contains all the KPIs of the requirements of the SMS
2. (Conception of current safety level) displays the level of efficiency of the requirements
3. (Actions) contains the proposed actions to be executed based on the efficiency levels

Following the PDCA process, in the “Plan” phase three different probability sets must be defined. In the sub-model 1 (Input information), the probabilities for the statuses included in each KPI must be defined. In the sub-model 2 (Conception of current safety level), the probabilities of efficiency and inefficiency of the requirements analysed by the indicator(s) must be defined considering the statuses of each KPI included in the assessment of the requirements. In the sub-model 3 (Actions), the probabilities for each recommended action must be defined based on the efficiency level of the requirements.

The probabilities are defined based on an evaluation of the common occurrence of the event analysed by the KPI. For example, if the KPI monitors the percentage of the vessels reporting when entering a VTS area, the probabilities of the KPI are defined as follow: more than 95%

(approximately 99% of the vessels based on VTS reports), less than 95 but no less than 75 (approximately 0.99% of the vessels based on VTS reports), and less than 75% (less than 0.01% based on VTS reports). For defining the probabilities in sub-models 2 and 3, the VTS managers make an anticipated evaluation of each status of these variables. Continuing with the same example, defining the probability of efficiency highly depends on having more than 95% of the vessels reporting when entering a VTS area, and defining the probability of inefficiency depends on having less than 95% of the vessels reporting. With the same approach, the definition of probabilities of each action depends on the probability of efficiency/inefficiency, giving maintenance and improvement actions when the requirement is efficient and detailed correction actions when it is inefficient.

In the “Do” phase, the outcome of the measured KPIs should be reported by including the evidence of the statuses resulted after the actual measuring of the KPIs. Evidence should be assigned to each variable representing the KPIs of the sub-model 1 (Input information). In the “Check” phase, the probability levels on the efficiency and inefficiency of the requirement based on the included evidence in each KPI should be reviewed. All variables presenting the level of efficiency of each requirement are included in the sub-model 2 (Conception of current safety level). Furthermore, the “Check” phase continues with the review of the produced probability levels registered in the recommended actions appointed to each requirement in the sub-model 3 (Actions). As part of the “Act” phase, the actions with the higher registered probability in each requirement represent the ones that should be executed.

4. Case study

In this section, a case study conducted in Vessel Traffic Services (VTS) in Finland is presented. VTS Finland represents the system and context in which the proposed process to design and implement SMS is applied. VTS is a worldwide actor responsible for monitoring and controlling the safety and smooth development of maritime traffic (Praetorius et al., 2015). Previously, work questioning the actual role of

VTS as safety controller has been presented in (Praetorius et al., 2015; Praetorius and Hollnagel, 2014; Westrenen and Praetorius, 2012). These studies discuss the importance of understanding the performance of socio-technical systems and the effect of system variances on the actual output of the system performance. This represents a common aim included in the objectives of this study.

4.1. VTS in Finland

4.1.1. VTS Finland system background

The competent authority of VTS Finland is the ministry of transport and communications. In the practice, the Finnish Transport Agency (Liikennevirasto) is the designated VTS authority in Finland (FTA, 2016). VTS Finland provides services for monitoring, communicating and reporting any event or issue related to the maritime traffic in seven areas monitored and controlled by the three established VTS centres. These areas are Bothnia VTS, West Coast VTS, Archipelago VTS, Hanko VTS, Helsinki VTS, Kotka VTS and Saima (Saima lake region) VTS. The VTS centres are Gulf of Finland VTS, Western Finland VTS and Saima VTS. Moreover, Finland VTS is complemented with the management of the mandatory ship reporting system in the Gulf of Finland (GOFREP), safety radio communication (Turku Radio) and the Traffic Separation Schemes in the Gulf of Finland and Åland Sea (FTA, 2016).

All vessels of 24 metres in length overall or more are obliged to participate in the vessel traffic services when navigating a determined Finnish vessel area. They are required to maintain a continuous listening and monitoring of the working channel used in the area. The general services provided by VTS Finland include:

- *Information*: this comprises information of the traffic conditions in the areas and the condition of the aids to navigation and channels.
- *Navigational assistance*: includes the provision of information about the vessel's position and bearings/courses over ground. It is provided at open sea, and from the open sea to the vicinity of pilot boarding places and also outer anchorages. It is only advisory and normative, the master of the vessel is the final responsible for its manoeuvring.
- *Traffic organization*: it prevents dangerous meeting, crossing and overtaking situations and congestion. For this, VTS separates the traffic in terms of time or distance according to the situation and circumstances, so that vessels are able to meet in a safe area.

The communication and provision of service in VTS centres are executed by VTS officers, their main tasks are the monitoring of vessel movements, organizing traffic in the areas and when necessary informing the vessels about any dangers. The information provided is based on the data received from radio communication and image from the radar and/or AIS system.

4.1.2. International Association of Lighthouse Authorities (IALA): VTS guidelines and recommendations

The International Association of Lighthouse Authorities (IALA) promotes coordination between different navigational stakeholders to create harmonised aids for worldwide navigation and to ensure the safe and efficient movements of vessels while protecting the environment (IALA, 2012). IALA publishes guidelines, handbooks, and recommendations for maritime navigation. In the case of VTS, IALA provides general guidance for the provision of Vessel Traffic Services in the VTS Manual (IALA, 2012). This manual establishes a standard for services offered at VTS centres and the basic requirements for the formation of VTS personnel (Praetorius et al., 2015). In this study, the guidelines and recommendations provided by IALA are considered for complementing the analysis of the actual safety function of VTS Finland.

4.1.3. VTS Finland Quality Management System

VTS Finland organizes and reviews the quality of the established processes that ensure the desired level of the functioning of the VTS centres. The Quality Management System (QMS) contains processes to analyse the entire function of the VTS Finland. These include routine processes, deviation process, special arrangements during wintertime, complementary VTS services, and support processes. Appendix A presents a general description of the integrated processes in the VTS quality management system and its connection with the international demands (guidelines) from IALA. These processes are considered for defining the basis of the SMS (Level 0).

4.1.4. VTS training provision

Training is an essential aspect considered for the design of the VTS Finland SMS. Each VTS centre must be operated with competent personnel. As first step in the analysis of the training provision, five IALA recommendations and guidelines are considered and reviewed:

- Standards for training and certification of VTS personnel (IALA Recom. V-103)
- The accreditation and approval process for VTS training (IALA Guideline 1014)
- Assessment of the training requirements for existing VTS personnel, candidate VTS operators, revalidation of VTS operator certificates (IALA Guideline 1017)
- Simulation in VTS training (IALA Guideline 1027)
- Train the trainer (IALA Guideline 1103)

In practice, the provision of training to VTS personnel is given by using two common alternatives. One, providing the on-the-job training. This is basically guided by VTS supervisors. This is a common and practical option to implement because new operators joining a centre are familiar with the operation of the VTS centre. Thus, “new” operators joining the centre have always a relevant background which enables the provision of training in a kind of “advanced” level. Two, providing training by using an alternative source (trainer facilitator). This option covers the elements that need to be strengthened in the formation of VTS personnel. This utilizes monitoring traffic simulators and other relevant environment simulators for analysing a particular context or issue of interest.

In this study, the analysis of the training courses provided for VTS personnel is executed (Aboa Mare, 2018). This includes participation in the VTS course V-103/1 arranged by Aboa Mare Maritime Training centre in Turku, Finland. The description of the course can be found in Aboa Mare (2018). The analysis includes the review of the materials and the context utilized in the training provision, including the interaction between trainers and trainees.

4.2. Designing a SMS for VTS Finland

4.2.1. VTS Finland program management (Level 0)

4.2.1.1. VTS Finland quality management system (task 0.1. In Fig. 4). The structure of VTS Finland Quality Management Systems is the basis for designing the SMS. This structure represents the point of reference for defining the initial expected characteristics of the SMS. For simplifying the presentation of the results derived from the application of the process to design the SMS in VTS Finland, in next sections, examples particularly linked to the routine process C “Provision of VTS” (see Appendix A) are presented. This process has the following aim:

- Provision of VTS begins when a vessel enters a VTS area. It covers the provision of the three services provided by VTS centres (see Section 4.1.1). This includes for example:
 - Sharing the information about the route to be monitored with the ship's master
 - Providing guidance for the routing of the vessel

Table 1
Definition of the main accidents affecting the function of VTS centres.

Accident type	Accident	Navigational season
Internal	1. Fire on the VTS centre	Both seasons
	2. Blackout in the VTS centre	Both seasons
	3. Technical failure	Both seasons
	3.1. Radar	
	3.2. Image monitoring system	
	3.3. Communications system	
External	4. Collision ship-to-ship	Both seasons
	4.1. In meeting	
	4.2. Passing	
	4.3. Crossing	
	4.4. In pilot assistance.	
	5. Collision with a fixed object	Both seasons
	6. Grounding	Both seasons
	7. Fire on board	Both seasons
	8. Loss of stability	Both seasons
	9. Machinery damage	Both seasons
	10. Accidental waste or oil spill	Both seasons
	11. Propeller damage	Both seasons
	12. Rudder damage	Both seasons
	13. Blackouts	Both seasons
	14. Collision ship-to-ship (winter navigation)	Navigation in ice conditions
	14.1. Collision during icebreaker assistance.	
	15. Hull damage due to ice contact (only significant noticed and reported damage which endangers the navigational safety)	Navigation in ice conditions
	16. Propeller damage	Navigation in ice conditions
	17. Rudder damage	Navigation in ice conditions
	18. Ship stuck in ice	Navigation in ice conditions
	19. Icing (icing which affects the execution of navigation)	Navigation in ice conditions
	20. Technical failures on board	Both seasons
	20.1. In radar	
	20.2. In screens	
	20.3. In communication devices	

- Informing about possible warnings in the ship's route (complex traffic and weather conditions, accidents, etc.)
- Informing about navigational conditions (wind, visibility, currents, waves, ice, etc.)
- Supporting on assistance operations (bearings, anchoring places, pilot services, icebreaker services, etc.)
- Organizing the traffic (e.g. guiding ships on crossing, overtaking and meeting)

4.2.2. Definition of the actual system goals and constraints (Level 1)

4.2.2.1. *Defined and identified accidents (task 1.1 in Fig. 4).* Accidents are categorized as internal or external. Internal accidents occur at the VTS centres, whereas external accidents occur in the maritime operations and these have repercussions in the functioning of the VTS centres. Table 1 presents a list of internal and external accidents categorized by the navigational season (navigation in open water and in sea ice conditions).

4.2.2.2. *Hazard identification (task 1.2 in Fig. 4).* In this study, the hazard identification is supported by the analysis of the work context in VTS centres. This includes visits to Western Finland VTS centre, discussions with operators and supervisors in this centre, and the analysis of the training provided for VTS personnel (see Section 4.1.4). Table 2 presents the identified hazards for the accidents presented in Table 1.

Table 2
Identified hazards in the functioning of VTS centres.

Hazard	Accident
A.1 Electrical equipment without proper maintenance	1
A.2 Flammable material not properly controlled	
A.3 Lighting during storm affecting electrical equipment	
A.4 Fire in neighbouring building and/or office	
B.1 Power grid failure	2
B.2 Electrical equipment without proper maintenance	
C.1 Radar equipment without proper maintenance	3
C.2 Image system (AIS) outdated and/or without proper maintenance	
C.3 Communication equipment (radio, telephone, and IT) without proper maintenance	
C.4 Weather causing failures (lighting storms, winter storms, heavy rain, heavy waving, and strong winds)	
D.1 VTS provide erroneous information to the vessel(s) in the area.	4–6; 14 and 16
D.2 VTS provide inappropriate navigational assistance (guidance) to the vessel(s) in the area.	
D.3 VTS set an erroneous organization of the vessels in the area.	
D.4 VTS interferes and affects communication between vessels when meeting, passing and crossing	
D.5 Inappropriate coordination of piloting services between the vessel, pilot and VTS.	
D.6 Inappropriate coordination and cooperation during assistance operations (SAR operations, Icebreaker)	
D.7 Inappropriate coordination with icebreakers.	
D.8 VTS centre is not capable of contacting a vessel (vessel no responding to radio communication)	
E.1 Vessels sailing over the speed limits set in a restricted area or channel	4; 5 and 6
E.2 Violation of the traffic separation schemes (TSS)	
F.1 Extreme weather conditions	3–6 and 14
F.1.1. Storms	
F.1.2. Heavy rain	
F.1.3 Heavy waving	
F.1.4 Strong winds	
F.1.5. Poor visibility	
G.1 Extreme weather conditions “wintertime”	4–6; 8; 14; 15; 16; 17; 18; 19 and 20
G.1.1 Winter storms	
G.1.2 Thick ice	
G.1.3 Ice ridges	
G.1.4 Strong winds	
G.1.5 Poor visibility	
G.1.6 Sea breeze	
G.1.7. Ice large floes	
G.1.8 Erroneous ballast of a vessel	
H.1 Sea bottom and rocks in shallow waters	6
I.1. Electrical installations on-board without proper maintenance	7 and 13
J.1 Machinery on-board without proper maintenance	4–7; 9; 10; 13; 14 and 18
K.1 Navigational and electronic devices without proper maintenance (on-board)	4; 5; 6; 14; 18 and 20

4.2.2.3. *Preliminary hazard analysis (task 1.3 in Fig. 4).* The evaluation of the effect between managing the risk of accidents and the cost of having a determined safety control is essential in the design of a SMS. This begins with this preliminary hazard analysis. Appendix B presents the preliminary analysis of hazards. It aims at assisting in identifying, listing and selecting a system architecture with fewest serious hazards and with the highest mitigation potential for the hazards that are not possible to eliminate. The analysis is complemented with a description of the hazard effect, its potential causal factors and mitigation actions. Table 3 presents the utilized format for complementing the preliminary hazard analysis. It presents the analysis of the hazard D.2 (VTS provide inappropriate navigational assistance to the vessel(s) in the area).

Table 3
Complementary hazard description and mitigation strategy.

Hazard	D.2 VTS provide inappropriate navigational assistance to the vessel(s) in the area.		
Hazard effect/description	<i>Provide extra details regarding the designate severity rating</i> This hazard may lead to accidents such as collisions and groundings. Major impact on the traffic may result because this outcome could affect the navigation of other ships. Major impact on the ship structure can occur in an accident produced by this action. Major impact on the environment can be produced e.g. due to accidental oil spills after a collision.		
Causal factors	<i>Describe the hazard as system state. What conditions could influence the effect of the hazard occurrence?</i> <ul style="list-style-type: none"> – Work overload to the operator providing the navigational assistance. – Inappropriate interpretation of the monitored context. – Lack of skills for efficiently providing guidance (including English language skills) 		
Mitigation strategy	<ul style="list-style-type: none"> – Setting of appropriate work schedule for the operators – Creating appropriate training programs 	<i>Cost/Difficulty</i> Medium High	<i>Priority (1–4)*</i> 3 3
Mitigation priority scale*	<i>Level</i> 4 3 2 1	<i>Description</i> Eliminate Prevent Control Reduce	<i>Detailed description</i> Complete elimination of the hazard Reduction of the likelihood that the hazard will occur Reduction of the likelihood that the hazard results in an accident Reduction of the damage if the accident occurs

4.2.2.4. *The documenting of environmental assumptions (task 1.4 in Fig. 4).* Environmental assumptions must be documented to each analysed hazard. The complete list of documented environmental assumptions for the other identified hazards is presented in Valdez Banda and Goerlandt (2017). In hazard D.2 (VTS provide inappropriate navigational assistance to the vessel(s) in the area), the assumptions are:

- EA/D.2/1. There is a list of information for each ship navigating in the area. It includes the ship general information, its planned route and its current location and status.
- EA/D.2/2. There is a common approach which restricts the communication between the VTS centre and the vessel to make it clearer and more efficient.
- EA/D.2/3. International guidelines and standards (IMO and IALA Guidelines) are considered to ensure the effectiveness of the provision of assistance.
- EA/D.2/4. The VTS operators and supervisors are trained in simulated environments to assess and improve the provision of navigational assistance.

4.2.2.5. *The initial restrictions of the SMS (task 1.5 in Fig. 4).* In the analysis of VTS Finland, three system restrictions are identified:

- VTS centres and operators provide information, guidance, assistance and support to organize traffic. However, pure commands are never provided, the final decision and responsibility remain in the vessel, its master and its crew.
- The interaction between VTS centres and vessels must not degrade the safety performance of the vessel. VTS operators should avoid the misleading of the vessel operation or provoke a wrong situational awareness for the vessel and the traffic.
- During navigation in ice conditions, VTS is restricted to monitor and support the operations of the vessels, including icebreaker operations. Icebreakers are the main responsible for providing information (e.g. location of waypoints) and on-site assistance.

4.2.2.6. *SMS requirements (task 1.6 in Fig. 4).* Table 4 presents the high-level functional requirements under the general objectives of the designed SMS for VTS Finland.

4.2.2.7. *Link between the system requirements and detected hazards (task 1.7 in Fig. 4).* Appendix C presents the links between the defined SMS requirements and the detected hazards.

4.2.2.8. *High-level safety constraints of the SMS (task 1.8 in Fig. 4).* Table 5 presents the identified safety constraints for the hazard D.2 (VTS provide inappropriate navigational assistance to the vessel(s) in the area). It presents the link between the system level requirements and the environmental assumptions. The complete list of the identified high-level safety constraints is presented in Valdez Banda and Goerlandt (2017).

4.2.3. Initial system design and analysis (Level 2)

4.2.3.1. *External interface, controls and displays, and logic principles for the functioning of the requirements of the SMS (task 2.1 in Fig. 4).* This includes how the requirements are executed in practice. Initially, it describes the external interface used for accomplishing the requirement purpose, including the identification of other organizations influenced by the requirement. Then, it describes the actual controls and displays used in the execution of the requirement and the functional logic principles. Table 6 presents the elements for the execution of the requirement (Req./G2/2). The other elements identified for each requirement are described in Valdez Banda and Goerlandt (2017).

4.2.3.2. *Validation and complete hazard analysis of the requirements (task 2.2 in Fig. 4).* This is the final step for validating the design of the requirements. The STPA is applied for the analysis of the hazards already identified in the preliminary analysis. The aim is to identify scenarios which may trigger the accidents. Table 7 presents an example of the application of the STPA for the analysis of the identified hazards in Level 1 for Hazard D.2 of Table 2.

4.2.4. System architecture, design, and physical representation (Levels 3–5)

4.2.4.1. *Architectural design and functional allocation (task 3.1 in Fig. 4).* Appendix D presents the map of the general goals of VTS Finland, the established SMS requirements in each goal, and the connection to the identified hazards.

4.2.4.2. *System design and physical representation (task 4–5.1 in Fig. 4).* In this study, processes for reviewing how the actual demands (needs of the system implementers and designers) are communicated to the component designers (e.g. subcontractor) are proposed. Table 8 presents a guide for reviewing the design and application of the VTS Finland traffic monitoring system.

4.2.5. System operations (Level 6)

4.2.5.1. *Auditing procedure (task 6.1 in Fig. 4).* The auditing procedure designed for the internal review of the VTS Finland SMS is based on the

Table 4
High-level functional requirements for the function of VTS Finland SMS system.

Goals/requirements	Definition
G1	Provide information when the vessels report to the centres or when vessels request it. This comprises information about the traffic conditions in the areas and the condition of the aids to navigation and channels.
Req./G1/1	15 min before entering a VTS area, vessels must provide its basic information (vessel name, location, destination, intended route and vessel condition) to VTS centre.
Req./G1/2	A traceable route is generated in the VTS traffic monitoring system to all the vessels entering a VTS area.
Req./G1/3	Once the vessel route is known, VTS operators must inform about warnings, traffic and weather conditions, and extraordinary events (e.g. accidents in the area).
G2	Provide navigational assistance to identify vessels on request or when considered necessary by the VTS centres. The intention is to support, with guidance, the smooth flow and safety of navigation.
Req./G2/1	Vessels navigating within a speed restricted area must respect the speed limits and keep their speeds within the established range.
Req./G2/2	A vessel approaching to a point of contingency must be informed about the situation and recommendations (guidance) should be provided.
Req./G2/3	Vessels in route of collision (detected with the use of the collision alarm in the VTS centre) must be contacted and informed about the risk.
Req./G2/4*	Vessels in convoys or escorted without the assistance of an icebreaker should be closely monitored in the VTS centres, and detected deviations must be reported to the icebreaker responsible for the area.
Req./G2/5	Vessels navigating in a route where a possible grounding could occur must be contacted and informed about the risk.
Req./G2/6*	Vessels navigating in a route where complex ice conditions can be foreseen must be informed about this situation and re-recommend the following of the waypoints.
G3	Traffic organization is given to prevent dangerous meeting, crossing and overtaking situations and traffic congestion. The aim is to improve traffic flow and ensure the safety of navigation.
Req./G3/1	Vessels must be informed of places and/or circumstances during navigation where/when meeting and overtaking is prohibited
Req./G3/2	For certain vessels and in certain navigational circumstances pilotage is compulsory. VTS operators must inform both the vessel and pilots.
Req./G3/3*	During wintertime, VTS centres should be aware about the type of vessel entering the areas and support the work of icebreaker with e.g. inform the vessel about its restrictions and providing the contact information of the icebreaker coordinator.
Req./G3/4*	During wintertime, meeting and overtaking is more common (e.g. in opened path channels in the ice). Moreover, distances between vessels are typically closer than in open water. VTS centres should closely monitor and support these operations.

* Particular requirements for wintertime navigation: navigation in ice conditions.

Table 5
The identification of the high-level safety constraints for hazard D.2.

Hazard D.2. VTS provide inappropriate navigational assistance to the vessels in the area.		
Environmental assumption	Requirements	Safety constraints (SC)
EA/D.2/1	Req./G2/2	SC. The IALA guidelines and recommendations are implemented in the functioning of all the VTS centres. These are applied and adapted to the needs of the maritime traffic in Finnish sea areas. This includes:
EA/D.2/2	Req./G2/3	– Acquisition of the most appropriate technology to provide VTS services all year around (including winter ice navigation).
EA/D.2/3	Req./G2/4	– The cooperation with all relevant stakeholders in the provision of navigational assistance (ships, pilots, icebreakers, authorities, etc.)
EA/D.2/4	Req./G2/6	– The safety and business strategy targets stated by VTS Finland and Finnish maritime authorities
		SC. VTS Finland periodically reviews the skills of the personnel of the centres.
		SC. The operators are trained to be efficient when providing navigational assistance. Demanded basic training by IALA is provided to operators and supervisors. The training is strengthened by having exercises in simulated environments which are evaluated by training experts.

IALA Guideline 1101 (Auditing and assessing VTS). This guideline focuses mainly on the review of the quality management of VTS. However, many sections of this guideline are connected with the management of safety. Based on this document, a personalized internal auditing procedure to review the designed SMS is proposed. This procedure is presented in Valdez Banda and Goerlandt (2017).

4.2.5.2. *Reviewing the skills of personnel in VTS Finland (task 6.2 in Fig. 4).* The analysis of VTS training provided by Aboa Mare Maritime Training Centre enabled the identification of different strengths and

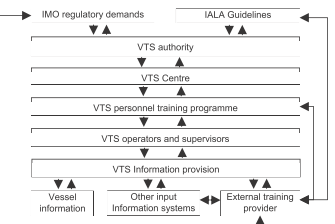
weaknesses detected in the performance of the VTS personnel. The best attribute of VTS personnel is the level of experience, knowledge and familiarization in the functioning of a VTS centre. This analysis demonstrates that VTS operators and supervisors have a clear understanding of the work context in VTS centres. Moreover, VTS personnel account with a fast and clear processing of the information. This includes the understanding of the functioning of the technology and equipment.

The biggest challenge for VTS personnel seems to be the manner operators execute the message markers. These should be simple, clear,

Table 6
Elements involved in the execution of the system requirement (Req./G2/2).

Req./G2/2. A vessel approaching to a point of contingency must be informed about the situation and recommendations (guidance) should be provided.	
External interface	Radio is the most common means used to inform about contingencies in the planned route. In case communication by radio is not possible, other alternatives must be used. The requirement could have connection with other organization such as pilots, icebreakers, SAR services, shipping company and any organisation affected by the logistics chain of the vessel.
Controls and displays	Vessels report contingencies to VTS centres via radio. This enables the marking and displaying of the areas of contingency within VTS traffic monitoring system.
Logic principles	Once contingencies are reported, marked and displayed in the VTS traffic monitoring system, VTS operators inform the potential risk to other vessels approaching the area and provide recommendations about how to proceed.

Table 7
Redefining the design of requirements and safety constraints of the SMS.

Hazard D.2 VTS provide inappropriate navigational assistance to the vessels in the area.
Safety Constraint to be refined
SC. The operators are trained to be efficient when navigational assistance is provided. Mandatory basic training by IMO and IALA is provided for VTS operators and supervisors. The training is strengthened by having exercises in simulated environments that are evaluated by training experts.
Control structure
 <p>This figure represents the control structure describing the most relevant components of the system where responsibilities, the constraints given between components, and feedback are graphically represented for analysing the hazard</p>

Detecting potentially Unsafe Controlled Actions (UCAs)

- UCA 1. The training of VTS personnel does not consider the demands and guidelines of the IALA normative.
- UCA 2. The training provided does not match the needs and characteristics of an actual service provision.
- UCA 3. The training does not efficiently consider the scope and limitations on the provision of navigational assistance.
- UCA 4. The training does not efficiently consider the common input from relevant information systems such as pilots, icebreakers, SAR services, tugs, weather services and the technology providers.
- UCA 5. The external training provider lacks understanding about the actual context of application and the actual skills to be trained.
- UCA 6. The methodology tools and technology implemented by the external training providers do not match the needs of the demands in the reality.
- UCA 7. There is not a complete evaluation of the actual competence of the hired training provider and there is not review of the quality and efficiency of the training received.

Redefining of the safety constraint

SC. The operators are trained to be efficient when providing navigational assistance. Demanded basic training by IALA is provided for operators and supervisors. The training is strengthened by having exercises in simulated environments which are evaluated by training experts. This includes:

- Basic training in IMO regulations (e.g. SCTW) and IALA guidelines are considered in the training.
- The training programme efficiently covers the specifications of the actual scope and limitation in the provision of navigational assistance by VTS Finland.
- Trainers incorporate the actual characteristics on the exchange of information between VTS centres and vessels, including the understanding about the common conflicts during communication.
- Trainers understand and incorporate the roles of relevant stakeholders to the training offered.
- The external training provider must be accredited and it should prove the understanding about the actual needs on the provision of VTS. For this, VTS is responsible for communicating and ensure that these aspects are included in the service provided by the outsourced entity.
- The provision of training is supported by having exercises in simulated environments which are evaluated by the responsible for the provision of training in VTS Finland.
- VTS Finland should perform a review of the efficiency and quality of the content of the training offered.

and appropriate. For example, when a vessel is violating the speed limits, instructions should be communicated in line with the system purpose and restrictions (see Section 4.2.2):

- M/S name: the speed limit in your area is 12 knots, adjust your speed to a reasonable speed. Thus, avoiding giving instructions such as: reduce your speed to 12 knots.

Table 9 presents the results of the strengths, weaknesses, opportunities and threats (SWOT) analysis elaborated after the review of the outcome of the VTS training course.

4.2.5.3. *Kpis of the designed VTS Finland SMS (task 6.3 in Fig. 4).* The definition of KPIs of the SMS is developed by executing the analysis of the context, mechanism, and outcome of the 13 requirements of SMS. Table 10 presents the analysis of the requirement Req./G2/2 to define its KPIs. The analyses of the other SMS requirements are presented in Valdez Banda and Goerlandt (2017). The analyses resulted in the definition of 31 KPIs for monitoring and reviewing the performance of the designed SMS. Appendix E presents the list of KPIs for monitoring the function of the SMS.

This analysis has also identified three dynamic system components which are essential for ensuring the functioning of the requirements and the VTS centres. These elements are:

- VTS personnel (particularly operators and supervisors)
- VTS traffic monitoring system
- VTS communication means

Ensuring the functionality of these components is essential. Therefore, the training of VTS personnel and the maintenance of VTS equipment are two aspects which demand performance monitoring and reviewing. Table 11 presents the KPIs for monitoring and reviewing the function of these components.

4.2.5.4. *SMS performance monitoring tool (task 6.4 in Fig. 4).* This task produced a tool for monitoring, reviewing and guiding the performance of the SMS requirements. It is used for the practical monitoring and reviewing of 31 KPIs. In addition, the tool assesses and recommends actions aiming at strengthening the functioning of the SMS. Table 12 presents an example of the practical content and functionality of the KPIs linked to the requirement Req./G2/2 (listed in Table 4).

Fig. 6 presents the graphical description of the function of the defined KPIs for the requirement Req./G2/2. The figure presents the application of the tool based on PDCA process described in Section 3.4. The entire description of the function of each KPI included in the designed SMS for VTS Finland is presented in Valdez Banda and Goerlandt (2017).

5. Discussion

5.1. System engineering for designing SMS

System engineering has the purpose of supporting the design and management of complex systems during their complete functional life (Blanchard, 2004). The main intention is to develop a good early planning of the requirements demanded for the proper functioning of the system. Therefore, system engineering is particularly efficient for developing and managing the work processes and methodological tools from their initial design phase.

In the case of SMS, system engineering provides elements to plan and design the management and control structures required for the correct functioning of the system. In this study, system engineering principles have been applied to define the system requirements and control constraints. These focus on understanding the actual interaction between the human and technical elements of the system. This interaction is essential as it influences the behaviour of the people interacting with the system.

The approach to designing the presented SMS follows the foundations of system theory, particularly the analysis of organizational hierarchy levels and their emergent properties. The designed SMS focuses on understanding how these levels are generated, what are the common boundaries and how these are linked. Moreover, the SMS focuses on defining the actual communication and control structure at

Table 8

Assessment of the design and implementation of the VTS Finland monitoring system. Aspects to be evaluated and reviewed with the technology and service providers linked to it.

1. General review of the requirements for the functioning of the designed SMS for VTS Finland	
Requirement	Status and support evidence
All	<ul style="list-style-type: none"> – Are the requirements informed and detailed explained to the provider? – Are the assumptions and hazards explained and reviewed with the provider? – Are the requirements fulfilled by the provider? – Are the general aspects of the traffic monitoring system improved after reviewing the requirements with the provider?
2. The requirements of the SMS are linked to the demands in IALA regulations. These include:	
IALA regulation	Condition evaluated
IALA Guideline 1056 (On the Establishment of VTS Radar Services)	– Are the demands of the regulation fulfilled?
IALA Guideline 1111 (Preparation of Operational and Technical Performance Requirements for VTS Systems)	– Is the connection between the requirements included in the regulations and the requirement of the SMS clearly specified?
IALA Recommendation V-125 (The use and presentation of symbology at VTS Centre)	<ul style="list-style-type: none"> – Are these documents monitored and reviewed? – What is the status of the opened corrective, preventive or improvement which are produced after the reviewing of these documents?

Table 9

SWOT analysis of the VTS operators/supervisor detected in the VTS training course.

Strengths:	Weaknesses:
<ul style="list-style-type: none"> – Strong background in maritime navigation – Practical experience in actual ship operations – Experience in the actual functioning of VTS – Strong knowledge of maritime contexts – Strong knowledge of the functioning of the equipment and technologies – Fast processing of information in different contexts 	<ul style="list-style-type: none"> – Usage of the message markers – Language proficiency and communication
Opportunities:	Threats:
<ul style="list-style-type: none"> – Improve the use of message markers by implementing exercises in simulated environments – Improve the efficiency of communication internally and externally – Creating more interactive exercises which include VTS environment and ship simulators – Provide training for executing appropriate risk analysis 	<ul style="list-style-type: none"> – Experience influences the role of the VTS operators when using the message markers (assuming how the operator would act in the same context) – Internally VTS operators speak local language. The communication with vessels is English. This sometimes causes problems in the fluency of the communication when internal and external communication are combined. – The reporting of extraordinary events is demanded in VTS centres. Reporting after a finalized work schedule may compromise the quality of the reports.

each hierarchy level. This enables the design of a SMS which can understand the functioning of the organization and how to incorporate the demands of safety regulations in the actual organizational safety management.

5.2. Designing maritime SMS based on the STAMP safety intent specification

Selecting the framework for designing the safety intent specification incorporated to the STAMP methodology has provided the identification of the most relevant safety management elements in each level of the organizational hierarchy. This enabled the design of a control structure for the management of safety-critical organizations such as VTS Finland.

Initially, the analysis of the established quality management system (Level 0) has enabled the identification, understanding and adaptation of the management structure and management general practices of the organization into the initial concept of the SMS.

The continuation of the design process (Level 1) provides the definition of the core safety elements that the system aims to manage. The analyses executed at this level identify the hazards and general issues that the system must control. For this, the structure of the system incorporates the detailed description of the events threatening the safety of the organization (VTS centres). The identified 20 accidents and 26

hazards (see [Tables 1 and 2](#)) aim to cover the most critical scenarios which must be prevented to ensure the functioning of VTS centres.

The prevention of these events is linked to the safety management practices of the organization which come from the safety goals of the organization and the demands on regulations. This is represented in the system environmental assumptions which support the identification of the requirements and safety constraints of the designed SMS. This resulted in 13 requirements (see [Table 4](#)) for executing the safety management in VTS Finland.

The tasks included at this level support the development of a simplified process to set the system requirements and constraints. The generated requirements represent a relatively simple set of demands which cover the provision of VTS in Finland. The foundations of the system requirements and constraints include the links to the actual practices (managerial and operational) used to mitigate the system hazards and to obtain the SMS goals.

The continuation of the process (Level 2) is essential for detecting stakeholders outside of the organization that are affected by the implementation of the 13 requirements. The description of each requirement is extended by identifying the controls and displays utilized in the actual performance of the VTS centres. This includes the definition of the logic principles behind the interaction of the SMS requirements (see [Table 6](#)).

This level also executes the redefinition and validation of the system

Table 10
Defining of KPIs with the method proposed in Valdez Banda et al. (2016b).

CMO	Query	Response	KPIs
Req./G2/2. A vessel approaching to a point of contingency has to be informed about the situation and recommendations should be provided.			
Context	<p>What is (are) the main organizational aspect (s) influenced by the implementation of this requirement?</p> <p>What are the tasks linked to the application of this requirement?</p> <p>What is the status of the main conditions in the organization for implementing the requirement?</p> <p>What and who are responsible for the requirement implementation and maintenance?</p> <p>What is the current link of the requirement with other norms and regulations?</p>	<p>VTS personnel, communication means and the VTS monitoring system.</p> <p>VTS operators monitoring the traffic and informing about contingencies.</p> <p>Detecting contingency areas and informing the vessel about these is properly done today.</p> <p>VTS centres and the vessels in traffic which need to update the status information.</p> <p>Link to the demands by IMO SOLAS convention and IALA guidelines.</p>	<p>Providing guidance once contingencies are detected is essential for supporting ships traffic and for ensuring their safety. Based on the CMO evaluation the following KPIs are defined:</p> <p>KPI/Req./G2/2(1): Warnings emitted to vessels regarding contingency points (Outcome KPI)</p> <p>KPI/Req./G2/2(2): Vessels directly affected by registered contingency points? (Monitor KPI)</p> <p>KPI/Req./G2/2(3): Actions developed to support the skills of VTS personnel for providing guidance? (Drive KPI)</p>
Mechanism	<p>Which are the main means for the requirement implementation?</p> <p>How is the requirement currently communicated inside and outside of the organization?</p> <p>How is the organization capable of ensuring the understanding of the importance of the requirement?</p> <p>How are the skills and capabilities of the responsible personnel are evaluated?</p> <p>How is the organization capable of ensuring the link between the requirement and other norms and regulations?</p>	<p>Communication means at the VTS centre and VTS personnel.</p> <p>VTS operators and supervisors communicate it to internal and external VTS stakeholders.</p> <p>The tasks of VTS operators and supervisors are clearly specified. Moreover, personnel are training for managing contingencies.</p> <p>The skills of VTS personnel are periodically reviewed.</p> <p>The design of SMS includes the demands in IMO regulations and IALA guidelines and recommendations.</p>	
Outcome	<p>What is the current fulfilment level of the requirement?</p> <p>What are the expected results derived from the implementation of the requirement?</p> <p>What are the possible negative aspects that could affect the requirement implementation?</p> <p>What kind of improvement can be obtained after implementing this requirement?</p>	<p>Areas of contingency are primary aspects to be handled by VTS centres. The fulfilment level of this requirement is good.</p> <p>A more efficient flow of ships traffic and reducing the complexity during contingencies.</p> <p>Reporting habits, such as late reporting or poor quality in reporting which affects the provision of VTS. Also, the lack of skills in contingency management.</p> <p>More efficient and safer traffic flow. Better contingency management and support.</p>	

requirements and constraints by utilizing a process revision tool (the STPA). This tool supports the strengthening of the basis in the design of the SMS with an augmented analysis of the requirement and constraints, including an extended review of the ways these mitigate the identified hazards (Dokas et al., 2013; Kazaras et al., 2012). STPA enables the mitigation of the analysed hazards in different causal scenarios. This creates a SMS which has the ability to face or avoid hazards without suffering a complete failure. This is an important aspect also mentioned in the concept of resilience engineering presented by

Hollnagel et al. (2008).

The next levels (Levels 3–5) provide a means to make a straightforward communication of the structure and the requirements of the SMS. The general map of the requirements of the system (see Appendix D) provides a simple description of the demands for mitigating the system hazards. This represents a convenient means to communicate the structure of the SMS with any system stakeholder. For supporting the design of the system physical representation, a detailed process for reviewing the content of the SMS with the provider of the ship traffic

Table 11
KPIs for monitoring and reviewing personnel training and equipment maintenance.

Component	KPI
Training (TR)	<p>Training and formation of VTS personnel</p> <ul style="list-style-type: none"> – KPI/TR (1): Reviewing and strengthening of the skills of VTS personnel (Monitor KPI) Understanding the needs and demands of the current function of VTS, together with the skills and profile of the personnel. – KPI/TR (2): Planning and reviewing the annual training programme (Monitor KPI) Planning the provision of VTS training based on needs and demands detected. – KPI/TR (3): Reviewing of the quality and efficiency of the training provided (Outcome KPI) Executing an assessment of the received trained which is performed between training provider, personnel trained and training manager.
Maintenance (MA)	<p>VTS traffic monitoring system</p> <ul style="list-style-type: none"> – KPI/MA (1): Executed maintenance programme for evaluating and ensuring the functionality of the traffic monitoring system and communication equipment (Outcome KPI) A maintenance programme is applied for the key equipment in the centres. Application and following of the programme is essential for ensuring their functionality. – KPI/MA (2): Reviewing the efficiency of the maintenance of the equipment (Monitor KPI) Assessing the received maintenance, including in-house and outsourced maintenance.

Table 12
Example of the content and functionality of the KPIs for Req./G2/2.

Req./G2/2	A vessel approaching to a point of contingency has to be informed about the situation and recommendations (guidance) have to be provided.
Current status and input information	<p>KPI/Req./G2/2(1) Warnings emitted to vessels regarding contingency points (OI[*]):</p> <ul style="list-style-type: none"> – Status A: Less than 5 warnings reported (in a determined time period) – Status B: Between 5 and 15 warnings reported – Status C: More than 15 warnings reported <p>KPI/Req./G2/2(2) Vessels affected by registered contingency points? (MI[*])</p> <ul style="list-style-type: none"> – Status A: Less than 3 vessels (in a determined time period) – Status B: Between 3 and 6 vessels affected – Status C: More than 6 vessels affected
Conceptual of current safety level of the requirement	<p>States for defining the current safety level:</p> <ul style="list-style-type: none"> – Efficient – Inefficient
Actions connected to the efficiency of the requirement	<ul style="list-style-type: none"> – Action A: Periodical reviews of the requirement and safety constraints linked to it. – Action B: Make a review of the requirement, including the analysis of the assumptions made to formulate it. Review the control structure established for analysing the hazards and unsafe controlled actions to make updates which improve the effectiveness on the transmission of warnings. – Action C: Make a detailed review of the preliminary hazard analysis to re-evaluate the relevancy of the detected hazards and discuss other potential threats connected with the function of the requirement. Complement this with the validation and complete hazard analysis using the STPA.
Actions from Drive KPIs (See Section 3.3)	<p>KPI/Req./G2/2(3) Actions developed to strengthen the skills of VTS personnel in the provision of guidance? (DI[*])</p> <ul style="list-style-type: none"> – Action A: Organize meetings and workshops to discuss issues influencing the effectiveness in the provision of warnings and navigational assistance. – Action B: Request for training to improve the emission of warnings and the provision navigational assistance. Analyse (with an outsourced organization) the conflicts in the emission of warnings and provision of navigational assistance.

* OI: Outcome Indicator, MI: Monitoring Indicator and DI: Drive Indicator.

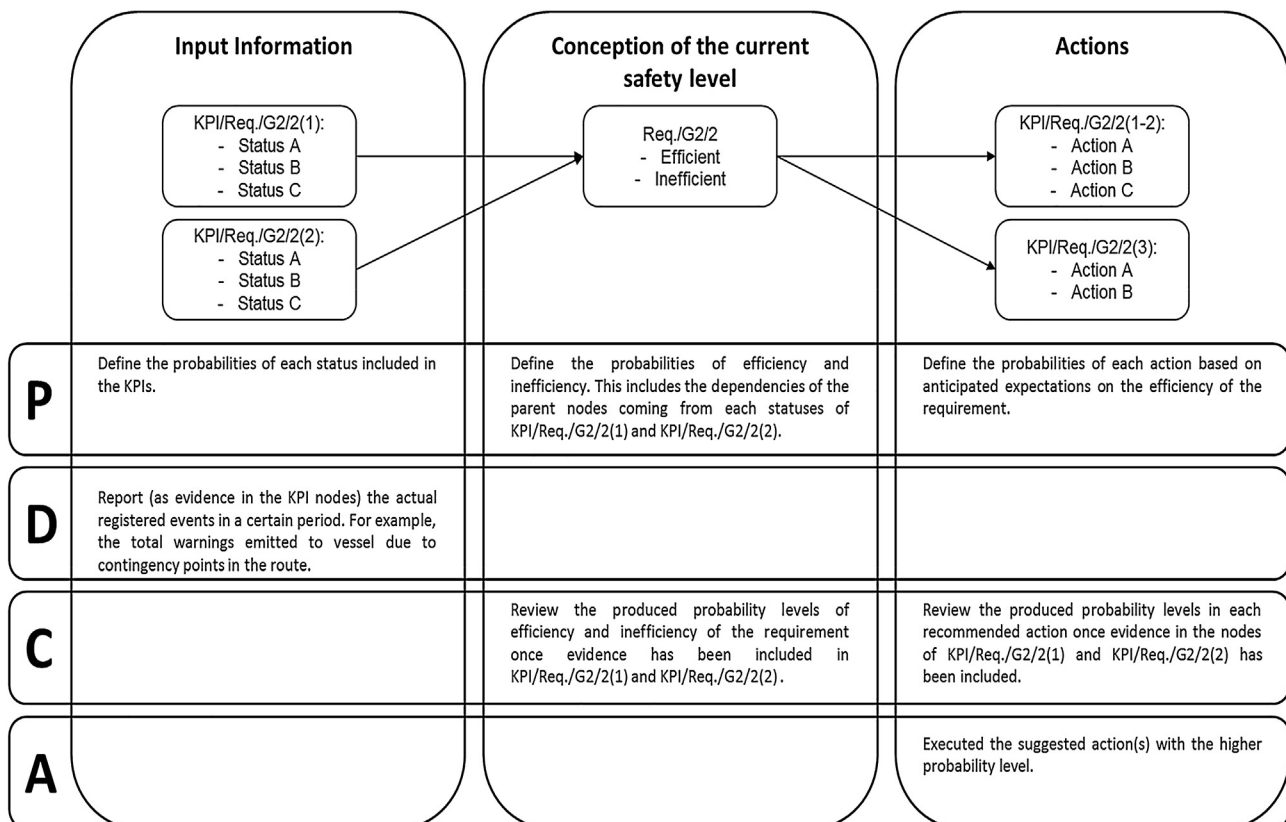


Fig. 6. Functioning of the performance monitoring tool based on the application of the PDCA process. It exemplifies the functioning of the KPIs of the requirement Req./G2/2.

monitoring system is proposed (see Table 8). The idea is to represent a guided review process that must be implemented to those software, equipment and service providers which contribute to the functioning of the SMS. This enables the integration of the SMS requirements and constraints on the tools utilized for completing the operations of VTS centres.

The culmination of the process for designing SMS (Level 6) focuses on the provision of process and tools for monitoring, reviewing and updating the functioning of the SMS. Initially, a structured internal audit process for reviewing the SMS has been proposed (Valdez Banda and Goerlandt, 2017). The process adopts the demands established in the regulations by IALA and simultaneously review the complete structure of the designed SMS.

The analysis at this level identifies the strengths and areas of opportunity in the performance of VTS operators and supervisors (see Table 9). Strong practical knowledge and understanding of the traffic operations and the practices implemented for monitoring ship traffic is the best quality of VTS personnel. The transmission of message markers and the alignment of communication practices internally and externally are the detected areas of opportunity. These findings are relevant to further develop new training strategies for VTS personnel. VTS personnel considers training as an exceptional context of analysis where mistakes are permitted and there is plenty of room for discussion and mutual learning.

This level also applies a process for identifying KPIs which can measure the performance of the system (see Table 10). The utilized method provides a systemic review of the requirements of the SMS. This is essential to understand the function of the KPIs and their contribution to the functioning of the SMS. The utilized method suits the general aim of the presented process for designing maritime SMS because it supports the definition of measurements for reviewing the SMS performance by analysing the assumptions behind each KPI. The combination of the assumptions behind the requirements of the SMS and the assumptions behind the KPI creates a systemic strengthening of the foundations of the SMS.

The last task of Level 6 offers a practical tool for monitoring and reviewing the performance of the designed SMS. This tool provides a systemic application of the KPIs. The functioning of the tool applies a Plan-Do-Check-Act (PDCA) process which is familiar to organizations aiming at controlling and improving the general management of their product or service offering. The tool initially supports the planning of the expected outcome of the SMS by anticipating (with the definition of probabilities) the results of the KPIs. It enables the incursion of the results obtained from the actual measuring of the KPIs. This allows comparison between the expected (defined probabilities of the KPIs) and real results (the actual reporting of the KPIs) to generate the level of efficiency in each requirement. Based on this level, the tool prioritizes certain action to correct, maintain, and improve the performance of the SMS.

In general, the proposed design process provides a guide to define the main structure and content of the SMS. The seven levels cover the most critical elements of safety management that need to be included in a system capable of developing and ensuring the safety strategy of VTS Finland. In the execution of this method, the most challenging aspects are the amount of information to be processed, and time invested in the development of each task of the process. This may lead to face some barriers when the available information is scarce or extensive, and the time for analysis is not enough. Therefore, the implementation of the process requires an adequate planning of the tasks with a defined time schedule. Furthermore, the planning and execution of the process demand the involvement of the actual VTS personnel. They represent the main reference to ensure the design of an efficient SMS for VTS Finland. For this, they need to count with adequate resources (knowledge, time, and supportive tools) for ensuring a positive outcome of the process application.

5.3. Limitations

5.3.1. Process limitations

The main limitation on the foundations of the STAMP safety intent specification is the setting of the level of details that the process aims to cover (Hardy and Guarnieri, 2011). This is also transferred to the process proposed for designing maritime SMS. This level of details is based on the safety goals and strategy adopted in the organization. This represents a complicated task because the organization needs to clearly define the resources available for designing the system. This creates a limitation for system designers and engineers who must carefully consider the available resources in the organization to execute and lead the list of tasks included in the process. Furthermore, the overall control structure of the SMS at different levels of the organization need to be finalized. The safety intent specification focus on the development of the system safety goals and requirements. However, the task to define the organizational processes and controls that implement these goals and requirements need to be executed once the designed structure of the SMS is validated.

5.3.2. Validation

The designed structure and content of the SMS for VTS Finland are not yet validated. However, a validation process has already been defined and applied together with operators, supervisors and managers at VTS. Once the analysis of the results derived from the process application is completed, the process and its application will be presented in Valdez Banda et al. (2018). This validation is essential to continue the development and posterior implementation of the SMS. This provides an overall estimation of the function of the SMS in terms of analysis and actual representation of the management of safety in VTS Finland. It focuses on validating if the designed SMS structure provides a good representation of the actual safety management in the organization. This assesses the feasibility of the SMS to continue its development and define the organizational processes and controls which guide the safety management practices at the different hierarchical level of the organization to achieve the safety management strategy of VTS Finland.

Another limitation is the lack of means and processes to validate the efficiency of the system once it is implemented. Today, SMS are applied in almost any safety critical organization. However, there are no concrete proofs which demonstrate the real benefits of having organizational SMS. This issue has previously been discussed in other studies (Dekker, 2004; Guastello, 1993; Hollnagel et al., 2008; Oltedal, 2009). However, industry sectors such as nuclear, aviation, railway and maritime have evidenced a progress in the safety performance by implementing and continuously improving their safety culture, safety management practices, and SMS (Celik, 2009; Clarke, 1998; Hetherington et al., 2006; Liou et al., 2008; McDonald et al., 2000; Rasmussen, 1997).

5.4. Future work

The reliability and validity of the proposed process are currently unknown. Future work should be focused on the development of appropriate frameworks for validating the initial structure and the posterior development, implementation, maintenance, and improvement of the designed SMS. The validation has to be done by those responsible for the safety management at VTS Finland. This provides elements to review the reliability of the analyses executed in the design method, focusing on obtaining arguments for an inter-subjective agreement of the outcome of these. This is a key issue previously pointed out in the implementation STAMP in Sharples (2017) and Kee et al. (2017). The study points out that in the analyses of the Sewol accident presented in Kwon (2016) and Kim et al. (2016), both analyses utilized STAMP and these have produced two different control structures for ensuring safety within the same context.

The validation of the initial structure of the designed SMS provides a

sustained argument for continuing the development of the SMS. This focuses on defining the adequacy of the SMS for supporting the VTS Finland safety policy and the function of the SMS for guiding the organizational safety management practices and assessing the potential benefits and challenges of the SMS for the actual organizational management. One clear needed step for this is the identification and definition of organizational processes and controls. These need to be defined depending on their purposes, either defining controls utilized to keep the system safe (state control) or defining controls to transfer the system back to a safe state when safety violations have occurred (Wahlström and Rollenhagen, 2014).

The validation of the SMS focuses on confirming that it efficiently manages and improves the safety performance of the organization and if it can also generate tangible benefits in the operation of organization. In the context of the process proposed in this study, this is an essential task for confirming the importance of investing resources and efforts since the initial design phase of the SMS. This includes the elaboration of analysis to represent the balance between the invested resources (money, time and people) and the actual benefits obtained (monetary and organizational competitive advantage).

6. Conclusion

This study presents a system and safety engineering process for designing maritime SMS. This process is proficient in adopting the actual safety practices of the organization and transferring these into the functioning of an organizational SMS. Simultaneously, the process is capable of adapting the demands on regulations into the functioning of the SMS. Thus, the process provides guidance to elaborate a set of demanded tasks to design SMS with a solid foundation in its structure.

The process is applied to design a SMS of VTS Finland. The aim is to develop the requirements and control constraints which can govern and guide the functioning of VTS centres with the purpose of ensuring the safety of ship navigation in Finnish sea areas. This has resulted in the

design of 13 safety requirements which contain the definition of the control constraints utilized to manage the safety of ship traffic in Finnish sea areas all year around.

In the application of the proposed process different tools have been provided to review the safety performance of the SMS and to revise the objectives and general functioning of the SMS with internal and external stakeholders. In general, the process provides several procedures and tools for planning the design of a SMS which can be posteriorly executed and maintained in a smooth and systemic manner. This aims at preventing unpredicted and expensive modifications afterwards.

In general, the proposed process and its application provide a systematic identification of key aspects that need be ensured in the management of safety at VTS. This systematic identification is essential for understanding the constitution of the safety management practices within an organization, incorporating a clear trace of these practices among the organizational structure. This is reflected in obtaining a clear and systematic description of the safety management in VTS Finland, providing details for developing, implementing, and maintaining the aspects of the safety management strategy linked to the designed SMS.

Acknowledgements

The work presented in this article is part of the research project “Strategic and Operational Risk Management for Wintertime Maritime Transportation System” (BONUS STORMWINDS). This project has received funding from BONUS, the joint Baltic Sea research and development programme (Art 185), funded jointly from the European Union’s Seventh Programme for research, technological development and demonstration and from the Academy of Finland. The authors want to thank the Finnish Transport Agency (Liikennevirasto) for its essential support and feedback for executing this study, and also express our gratitude to NOVA University of Applied Science for allowing our participation and analysis of the VTS course.

Appendix A. Process included in VTS Finland quality management system (see Section 4.2.1)

Process	IALA guideline
<i>Routine processes</i>	
A. Identification of ships entering the area Process for identifying and monitoring those vessels entering certain VTS area.	1056; 1111; 1089; 1105; 1083; 1102; 1071; V-127; V-103
B. Identification of ships leaving port Process applied for identifying and monitoring those vessels leaving port.	1089; 1083; 1102; 1071; V-127
C. Provision of VTS The process is activated when the process 1 or 2 started. This includes ship’s route to be monitored, routing the vessel, warnings, navigational conditions, assistance requests and organizing traffic in general	1089; V-127
D. The Gulf of Finland Reporting System (GOFREP) This is used for monitoring purposes depending on the navigational operations existing at the Gulf of Finland. It includes the reporting of deviations.	1018; V-127
E. Aland Sea Traffic Separation Schemes (TSS) The process attempts to ensure a safe navigation in this area where restrictions are set based on the complexity of this navigational section.	1105; 1110; 1071; V-127
F. Piloting This process is for transferring information to the pilot for performing its duties.	1102
<i>Deviation processes</i>	
G. Reporting of deviations Process for reporting deviations identified during traffic monitoring. Thus, VTS must intervene in the case of alerts and reported extraordinary events.	1111; 1089; 1102; 1071; 1110; 1018; V-127
H. Safety device fault recognition The process defines the actions to be taken if there any problem with the aids for navigations e.g. buoys and lighthouses.	1111
I. Places of refuge This process supports the problems and emergencies of the vessels navigating the area, and the designation of places for solving the problem affecting the vessel.	1110; 1071; 1089; V-127
J. Internal deviations in the VTS centres The process refers to technical problems or emergencies in the VTS centres	1110; 1111; 1018

- K. Deviations in piloting This manages and supports any unusual event during piloting services. 1102
- Arrangements during wintertime*
- L. Arrangement and management of waypoints The icebreaker coordinator of an area set/decide the waypoints and inform this to the VTS. VTS communicate this to the vessels in the area. 1102; 1018
- M. Modification of the Traffic Separation Schemes (TSS) This process describes the removal of TSS (depending on the ice conditions). 1102; 1110; 1071; 1018; V-127
- N. Agreement on the use of tug boats The process describes the using of tug boats for opening fairways in ice conditions. 1102; 1018
- O. Opening channel paths in coastal areas of the Gulf of Finland (GOF) Process is implemented when ice conditions are extreme in the GOF. 1102; 1018; 1089; V-127

Turku radio

- P. Turku radio (marine warnings and weather reports) This process provides aids for navigation (e.g. information about buoys, traffic and weather reports, ice reports, icebreaker locations and waypoints). 1089; 1018; V-127
- Q. Turku radio (emergency treatment) This process describes the management of emergency situations via Turku radio, including coordination with SAR services and any relevant stakeholder. 1089; 1018; V-127

Supportive processes

- R. Feedback reception and processing This process ensures that feedback is provided to any stakeholder when necessary. 1089; 1018; V-127
- S. Adapting changes in regulations. The process ensures that changes in regulations are analysed and adopted. 1018; 1089; 1102; V-127
- T. Developing training and competences The process describes the arrangement made by VTS Finland to ensure that VTS personnel is competent and properly trained. 1032; 1017; 1027; 1014; V-103; V-127

Appendix B. Analysis of the severity and likelihood of the identified hazards (see Section 4.2.2)

B.1. VTS Finland hazard analysis

Hazard	Severity				Likelihood
	H	T	E	P	
A.1	3	1	2	4	Low
A.2	3	1	2	4	Low
A.3	2	1	2	3	Low
A.4	3	1	2	3	Low
B.1	1	1	1	2	Medium
B.2	2	1	1	2	Low
C.1	1	3	1	2	Low
C.2	1	3	1	1	Low
C.3	1	2	1	1	Low
C.4	1	2	1	2	Medium
D.1	3	3	3	3	Low
D.2	3	3	3	3	Low
D.3	3	3	2	2	Low
D.4	2	3	2	3	Low
D.5	2	3	2	2	Low
D.6	4	3	3	4	Low
D.7	2	2	3	2	Low
D.8	4	3	3	4	Medium
E.1	4	3	4	4	Medium
E.2	4	3	4	4	Low
F.1					
F.1.1	3	3	4	4	Medium
F.1.2	2	2	2	1	High
F.1.3	2	2	2	2	Medium
F.1.4	2	3	2	3	Medium
F.1.5	3	3	4	4	Medium
G.1					

G.1.1	3	3	2	3	High
G.1.2	2	3	2	2	High
G.1.3	2	3	2	2	High
G.1.4	2	3	2	2	Medium
G.1.5	3	3	4	4	Medium
G.1.6	2	1	1	3	High
G.1.7	3	3	3	3	Medium
G.1.8	1	2	2	3	Medium
H.1	4	3	4	4	Medium
I.1	4	2	3	4	High
J.1	4	2	3	3	High
K.1	3	2	3	3	Medium

B.2. Description of the severity levels in the hazard analysis

Severity level	H Human	T Traffic operations	E Environment	P Property
4	Loss of life	Traffic operations discontinued	Catastrophic impact to the environment	VTS centre/ship loss
3	Severe injury or illness	Major impact to the operations	Major impact to the environment	VTS centre/ship major damage
2	Minor injury or illness	Minor impact to the operations	Minor impact to the environment	VTS centre/ship minor damage
1	Insignificant injury or illness	Insignificant impact to the operations	Insignificant impact to the environment	VTS centre/ship insignificant damage

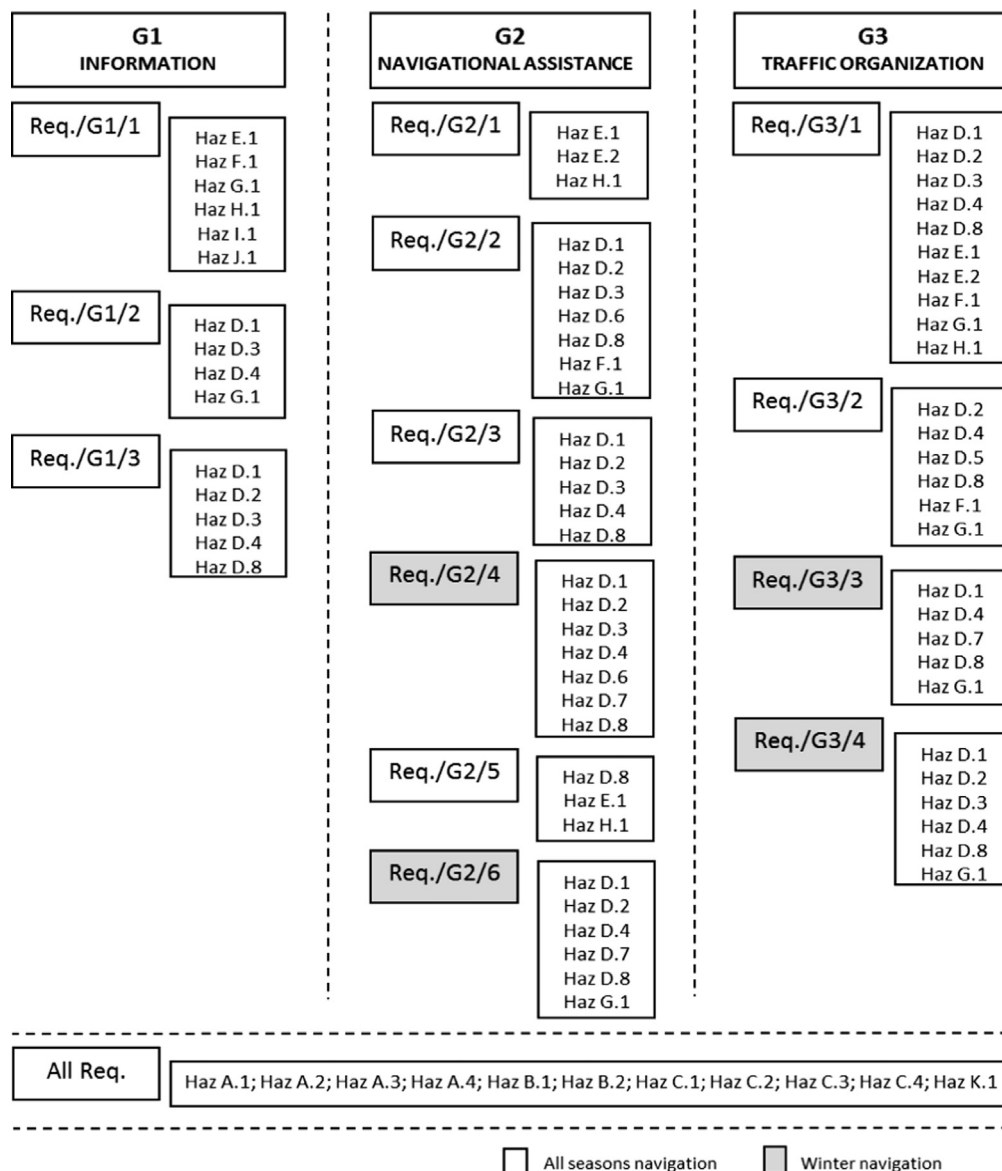
B.3. Description of the likelihood in the hazard analysis

Likelihood	Description
High	Frequent events
Medium	Occasional events
Low	Isolated/unlikely events

Appendix C. The link between the SMS requirements and hazards (see Section 4.2.2)

Requirement	Hazard																		
	A	B	C	D.1	D.2	D.3	D.4	D.5	D.6	D.7	D.8	E.1	E.2	F.1	G.1	H.1	I.1	J.1	K.1
Req./G1/1	X	X	X									X		X	X	X	X	X	X
Req./G1/2	X	X	X	X	X	X	X				X			X	X				X
Req./G1/3	X	X	X	X	X	X	X				X								X
Req./G2/1	X	X	X									X	X			X			X
Req./G2/2	X	X	X	X		X			X		X			X	X				X
Req./G2/3	X	X	X	X			X				X								X
Req./G2/4	X	X	X	X			X		X	X	X								X
Req./G2/5	X	X	X	X			X			X	X					X			X
Req./G2/6	X	X	X	X	X		X			X	X				X				X
Req./G3/1	X	X	X	X			X				X	X	X	X	X	X			X
Req./G3/2	X	X	X		X		X	X			X			X	X				X
Req./G3/3	X	X	X	X						X	X				X				X
Req./G3/4	X	X	X	X			X			X	X				X				X

Appendix D. Map presenting the general goals of VTS Finland, the SMS requirements in each goal, and the connection to the identified hazards (see Section 4.2.4)



Appendix E. KPIS of the VTS Finland SMS (see Section 4.2.5)

KPIs per requirement

1. KPI/Req./G1/1(1): Percentage of vessel reporting when entering a VTS area (if possible classified by VTS areas) (Monitor KPI)
2. KPI/Req./G1/1(2): Actions developed to improve the vessel reporting (in each VTS area) (Drive KPI)
3. KPI/Req./G1/1(3): The initial status of vessels when entering VTS areas is commonly (Outcome KPI)
4. KPI/Req./G1/2(1): Percentage of efficiency of the VTS monitoring system to represent (portray) ship routes? (Monitor KPI)
5. KPI/Req./G1/2(2): Reported malfunctions compromising AIS? (Outcome KPI)
6. KPI/Req./G1/3(1): Efficiency of the actions made by VTS to ensure vessels listen to the VHF channels? (Monitor KPI)
7. KPI/Req./G1/3(2): Actions developed to improve the information sharing in VTS (Drive KPI)
8. KPI/Req./G2/1(1): Reported speed violations occurred in VTS areas (Monitor KPI)
9. KPI/Req./G2/1(2): Actions made by VTS to efficiently inform about existing restricted areas? (Drive KPI)

KPIs per requirement

10. KPI/Req./G2/2(1): Warnings emitted to vessels regarding contingency points (Outcome KPI)
11. KPI/Req./G2/2(2): Vessels directly affected by registered contingency points? (Monitor KPI)
12. KPI/Req./G2/2(3): Actions developed to strengthen the skills of VTS personnel in the provision of guidance? (Drive KPI)
13. KPI/Req./G2/3(1): Warnings emitted to prevent close quarter situations/too small CPAs? (Monitor KPI)
14. KPI/Req./G2/3(2): Number of actual collisions reported? (Outcome KPI)
15. KPI/Req./G2/3(3): Actions developed to strengthen the skills of VTS personnel in the handling of the demanded tasks after a collision alarm is registered? (Drive KPI)
16. KPI/Req./G2/4(1): Navigational assistance provided to ships formed in convoys where icebreaker is not present? (Monitor KPI)
17. KPI/Req./G2/4(2): Reported incidents in convoys where icebreaker is not present? (Outcome KPI)
18. KPI/Req./G2/4(3): Reported accidents in convoys where icebreaker is not present? (Outcome KPI)
19. KPI/Req./G2/4(4): Joint actions between VTS and icebreakers to support winter navigation operations? (Drive KPI)
20. KPI/Req./G2/5(1): Ships detected and contacted due to potential drifting to the edge of a fairway? (Monitor KPI)
21. KPI/Req./G2/5(2): Vessels with a late response when these are contacted due to the risk of collision or groundings? (Monitor KPI)
22. KPI/Req./G2/5(3): Groundings reported within areas of the VTS Finland? (Outcome KPI)
23. KPI/Req./G2/6(1): Warnings emitted to vessels regarding difficult ice conditions and for recommending to follow the WPs? (Monitor KPI)
24. KPI/Req./G2/6(2): Request made to vessel for cutting off another vessel from ice (icebreakers are not involved)? (Monitor KPI)
25. KPI/Req./G3/1(1): Number of accidents registered in conditioned navigational areas? (Outcome KPI)
26. KPI/Req./G3/1(2): Type of actions executed to strength the traffic organization in the VTS centres? (Drive KPI)
27. KPI/Req./G3/2(1): Incidents during the coordination and initial provision of pilotage services? (Outcome KPI)
28. KPI/Req./G3/2(2): Type of actions executed to strength the cooperation between VTS and Pilots? (Drive KPI)
29. KPI/Req./G3/3(1): Interventions to guide and organize the traffic during wintertime (navigation in ice conditions)? (Monitor KPI)
30. KPI/Req./G3/4(1): Operations monitored due to their complexity? (Outcome KPI)
31. KPI/Req./G3/4(2): Navigational assistance caused by the characteristics of the operation and ice conditions? (Drive KPI)

References

- Aboa Mare, 2018. VTS Course: VTS Operator Basic URL < <http://www.aboamare.fi/VTS-course> > .
- Aps, R., Fetissov, M., Goerlandt, F., Helferich, J., Kopti, M., Kujala, P., 2015. Towards STAMP based dynamic safety management of eco-socio-technical maritime transport system. *Procedia Eng., Proceedings of the 3rd European STAMP Workshop 5-6 October 2015, Amsterdam* 128, 64–73. [10.1016/j.proeng.2015.11.505](https://doi.org/10.1016/j.proeng.2015.11.505).
- Aps, R., Fetissov, M., Goerlandt, F., Kopti, M., Kujala, P., 2016. STAMP-Mar based safety management of maritime navigation in the Gulf of Finland (Baltic Sea). In: 2016 European Navigation Conference (ENC). Presented at the 2016 European Navigation Conference (ENC), pp. 1–8. 10.1109/EURONAV.2016.7530538.
- Blanchard, B.S., 2004. *System Engineering Management*. John Wiley & Sons.
- Boström, M., Österman, C., 2016. Improving operational safety during icebreaker operations. *WMU J. Marit. Aff.* 1–16. [http://dx.doi.org/10.1007/s13437-016-0105-9](https://doi.org/10.1007/s13437-016-0105-9).
- Celik, M., 2009. Designing of integrated quality and safety management system (IQSMS) for shipping operations. *Saf. Sci.* 47, 569–577. [http://dx.doi.org/10.1016/j.ssci.2008.07.002](https://doi.org/10.1016/j.ssci.2008.07.002).
- Chatzimichailidou, M.M., Dokas, I.M., 2015. The risk situation awareness provision capability and its degradation in the Überlingen accident over time. *Procedia Eng., Proceedings of the 3rd European STAMP Workshop 5-6 October 2015, Amsterdam* 128, 44–53. [10.1016/j.proeng.2015.11.503](https://doi.org/10.1016/j.proeng.2015.11.503).
- Clarke, S., 1998. Safety culture on the UK railway network. *Work Stress* 12, 285–292. [http://dx.doi.org/10.1080/02678379808256867](https://doi.org/10.1080/02678379808256867).
- Conant, R.C., Ashby, W.R., 1970. Every good regulator of a system must be a model of that system. *Int. J. Syst. Sci.* 1, 89–97.
- Dekker, P.S., 2014. *The Field Guide to Understanding “Human Error.”* Ashgate Publishing, Ltd.
- Dekker, S., 2004. Ten Questions About Human Error: A New View of Human Factors and System Safety. CRC Press.
- Dokas, I.M., Feehan, J., Imran, S., 2013. EWASAP: an early warning sign identification approach based on a systemic hazard analysis. *Saf. Sci.* 58, 11–26. [http://dx.doi.org/10.1016/j.ssci.2013.03.013](https://doi.org/10.1016/j.ssci.2013.03.013).
- Ek, Å., Axelsson, R., 2005. Safety culture on board six Swedish passenger ships. *Marit. Policy Manag.* 32, 159–176. [http://dx.doi.org/10.1080/03088830500097455](https://doi.org/10.1080/03088830500097455).
- Falk, T., Rollenhagen, C., Wahlström, B., 2012. Challenges in performing technical safety reviews of modifications – a case study. *Saf. Sci.* 50, 1558–1568. [http://dx.doi.org/10.1016/j.ssci.2012.03.009](https://doi.org/10.1016/j.ssci.2012.03.009).
- Finnish Transport Agency (FTA), 2016. Vessel Traffic Services- Master Guides of the different VTS areas in Finland and the function of GOFREP reporting system and Turku Radio.
- Firesmith, D., 2004. Engineering safety requirements, safety constraints, and safety-critical requirements. *J. Obj. Technol.* 3 (3), 27–42.
- Fleming, C.H., Spencer, M., Thomas, J., Leveson, N., Wilkinson, C., 2013. Safety assurance in NextGen and complex transportation systems. *Saf. Sci.* 55, 173–187. [http://dx.doi.org/10.1016/j.ssci.2012.12.005](https://doi.org/10.1016/j.ssci.2012.12.005).
- Flin, R., Mearns, K., O'Connor, P., Bryden, R., 2000. Measuring safety climate: identifying the common features. *Saf. Sci.* 34, 177–192. [http://dx.doi.org/10.1016/S0925-7535\(00\)00012-6](https://doi.org/10.1016/S0925-7535(00)00012-6).
- Grote, G., 2012. Safety management in different high-risk domains – all the same? *Saf. Sci.* 50, 1983–1992. [http://dx.doi.org/10.1016/j.ssci.2011.07.017](https://doi.org/10.1016/j.ssci.2011.07.017).
- Guastello, S.J., 1993. Do we really know how well our occupational accident prevention programs work? *Saf. Sci.* 16, 445–463. [http://dx.doi.org/10.1016/0925-7535\(93\)90064-K](https://doi.org/10.1016/0925-7535(93)90064-K).
- Hänninen, M., Valdez Banda, O.A., Kujala, P., 2014. Bayesian network model of maritime safety management. *Expert Syst. Appl.* 41, 7837–7846. [http://dx.doi.org/10.1016/j.eswa.2014.06.029](https://doi.org/10.1016/j.eswa.2014.06.029).
- Hardy, K., Guarnieri, F., 2011. Using a systemic model of accident for improving innovative technologies: application and limitations of the STAMP model to a process for treatment of contaminated substances. In: *The 15th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2011*.
- Hetherington, C., Flin, R., Mearns, K., 2006. Safety in shipping: the human element. *J. Safety Res.* 37, 401–411. [http://dx.doi.org/10.1016/j.jsr.2006.04.007](https://doi.org/10.1016/j.jsr.2006.04.007).
- Hollnagel, E., Nemeth, C.P., Dekker, S., 2008. *Resilience Engineering Perspectives: Remaining Sensitive to the Possibility of Failure*. Ashgate Publishing, Ltd.
- Hollnagel, P.E., 2014. *Safety-I and Safety-II: The Past and Future of Safety Management*. Ashgate Publishing, Ltd.
- International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), 2012. *IALA Vessel Traffic Manual (5 ed.): International Association of Marine Aids to Navigation and Lighthouse Authorities*.
- Kazaras, K., Kiriopoulou, K., Rentizelas, A., 2012. Introducing the STAMP method in road tunnel safety assessment. *Saf. Sci.* 50, 1806–1817. [http://dx.doi.org/10.1016/j.ssci.2012.04.013](https://doi.org/10.1016/j.ssci.2012.04.013).
- Kee, D., Jun, G.T., Waterson, P., Haslam, R., 2017. A systemic analysis of South Korea Sewol ferry accident – striking a balance between learning and accountability. *Appl. Ergon.* Legacy Jens Rasmussen 59, 504–516. [http://dx.doi.org/10.1016/j.apergo.2016.07.014](https://doi.org/10.1016/j.apergo.2016.07.014).
- Kim, T.-E., Nazir, S., Øvergård, K.J., 2016. A STAMP-based causal analysis of the Korean Sewol ferry accident. *Saf. Sci.* 83, 93–101.
- Kristiansen, S., 2013. *Maritime Transportation: Safety Management and Risk Analysis*. Routledge.
- Kwon, Y., 2016. *System Theoretic Safety Analysis of the Sewol-ho Ferry Accident in South Korea*. Masters Thesis, MIT, USA. < <http://sunnyday.mit.edu/papers/Kwon-Thesis.pdf> > .
- Lappalainen, F.J., Kuronen, J., Tapaninen, U., 2014. Evaluation of the ISM code in the Finnish shipping companies. *J. Marit. Res.* 9, 23–32.
- Lee, S., Moh, Y.B., Tabibzadeh, M., Meshkati, N., 2017. Applying the AcciMap methodology to investigate the tragic Sewol Ferry accident in South Korea. *Appl. Ergon.* 59, 517–525.

- Leveson, N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.
- Liou, J.J.H., Yen, L., Tzeng, G.-H., 2008. Building an effective safety management system for airlines. *J. Air Transp. Manag.* 14, 20–26. <http://dx.doi.org/10.1016/j.jairtraman.2007.10.002>.
- Mayes, B.T., Allen, R.W., 1977. Toward a definition of organizational politics. *Acad. Manage. Rev.* 2, 672–678. <http://dx.doi.org/10.5465/AMR.1977.4406753>.
- McDonald, N., Corrigan, S., Daly, C., Cromie, S., 2000. Safety management systems and safety culture in aircraft maintenance organisations. *Saf. Sci.* 34, 151–176. [http://dx.doi.org/10.1016/S0925-7535\(00\)00011-4](http://dx.doi.org/10.1016/S0925-7535(00)00011-4).
- Øien, K., 2001. A framework for the establishment of organizational risk indicators. *Reliab. Eng. Syst. Saf.* 74, 147–167. [http://dx.doi.org/10.1016/S0951-8320\(01\)00068-0](http://dx.doi.org/10.1016/S0951-8320(01)00068-0).
- Olteidal, H., 2009. The use of safety management systems within the Norwegian tanker industry – do they really improve safety? In: Guedes Soares, C., Briš, R., Martorell, S. (Eds.), *Reliability, Risk, and Safety*. CRC Press.
- Olteidal, H., Wadsworth, E., 2010. Risk perception in the Norwegian shipping industry and identification of influencing factors. *Marit. Policy Amp Manag.* 37, 601–623. <http://dx.doi.org/10.1080/03088839.2010.514954>.
- Passenier, D., Sharpanskykh, A., de Boer, R.J., 2015. When to STAMP? A case study in aircraft ground handling services. *Procedia Eng., Proceedings of the 3rd European STAMP Workshop 5–6 October 2015, Amsterdam* 128, 35–43. [10.1016/j.proeng.2015.11.502](http://dx.doi.org/10.1016/j.proeng.2015.11.502).
- Pawson, R., Tilley, N., 1997. An introduction to scientific realist evaluation. In: Chelimsky, E., Shadish, W.R. (Eds.), *Evaluation for the 21st Century: A Handbook*. Sage Publications Inc, Thousand Oaks, CA, US, pp. 405–418.
- Pearl, J., 2014. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann.
- Praetorius, G., Hollnagel, E., 2014. Control and resilience within the maritime traffic management domain. *J. Cogn. Eng. Decis. Mak.* 8, 303–317. <http://dx.doi.org/10.1177/1555343414560022>.
- Praetorius, G., Hollnagel, E., Dahlman, J., 2015. Modelling Vessel Traffic Service to understand resilience in everyday operations. *Reliab. Eng. Syst. Saf. Spec. Iss. Resilience Eng.* 141, 10–21. <http://dx.doi.org/10.1016/j.res.2015.03.020>.
- Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. *Saf. Sci.* 27, 183–213. [http://dx.doi.org/10.1016/S0925-7535\(97\)00052-0](http://dx.doi.org/10.1016/S0925-7535(97)00052-0).
- Reason, J., 1997. Managing the Risks of Organizational Accidents. Routledge.
- Reason, J., 2005. Safety in the operating theatre – Part 2: Human error and organisational failure. *Qual. Saf. Health Care* 14, 56–60.
- Reason, J., 1998. Achieving a safe culture: theory and practice. *Work Stress* 12, 293–306. <http://dx.doi.org/10.1080/02678379808256868>.
- Reese, C.D., 2015. Occupational Health and Safety Management: A Practical Approach, third ed. CRC Press.
- Reiman, T., Oedewald, P., 2007. Assessment of complex sociotechnical systems – theoretical issues concerning the use of organizational culture and organizational core task concepts. *Saf. Sci.* 45, 745–768. <http://dx.doi.org/10.1016/j.ssci.2006.07.010>.
- Reiman, T., Pietikäinen, E., 2012. Leading indicators of system safety – monitoring and driving the organizational safety potential. *Saf. Sci.* 50, 1993–2000. <http://dx.doi.org/10.1016/j.ssci.2011.07.015>.
- Sarter, N.N., Woods, D.D., 1995. Strong, Silent, and Out-of-the-Loop. CSEL Report 95-TR-01. Ohio State University, February.
- Salmon, P.M., McClure, R., Stanton, N.A., 2012. Road transport in drift? Applying contemporary systems thinking to road safety. *Saf. Sci.* 50, 1829–1838. <http://dx.doi.org/10.1016/j.ssci.2012.04.011>.
- Schröder-Hinrichs, J.U., 2010. Human and organizational factors in the maritime world—are we keeping up to speed? *WMU. J. Marit. Aff.* 9, 1–3. <http://dx.doi.org/10.1007/BF03195162>.
- Schröder-Hinrichs, J.-U., Hollnagel, E., Baldauf, M., Hofmann, S., Kataria, A., 2013. Maritime human factors and IMO policy. *Marit. Policy Manag.* 40, 243–260. <http://dx.doi.org/10.1080/03088839.2013.782974>.
- Sharples, S., 2017. Commentary: analysis, investigation and judgement: the post-hoc application of human factors analyses to incidents. *Appl. Ergon.* 59, 526–527. <http://dx.doi.org/10.1016/j.apergo.2016.10.005>.
- Stringfellow, M.V., Leveson, N.G., Owens, B.D., 2010. Safety-driven design for software-intensive aerospace and automotive systems. *Proc. IEEE* 98, 515–525. <http://dx.doi.org/10.1109/JPROC.2009.2039551>.
- Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., Blokland, P., 2016. Process safety indicators, a review of literature. *J. Loss Prev. Process Ind.* 40, 162–173. <http://dx.doi.org/10.1016/j.jlp.2015.12.020>.
- Thomas, J., Suo, D., 2015. STPA-based method to identify and control feature interactions in large complex systems. *Procedia Eng., Proceedings of the 3rd European STAMP Workshop 5–6 October 2015, Amsterdam* 128, 12–14. [10.1016/j.proeng.2015.11.499](http://dx.doi.org/10.1016/j.proeng.2015.11.499).
- Valdez Banda, O.A., Goerlandt, F., Kuzmin, V., Kujala, P., Montewka, J., 2016a. Risk management model of winter navigation operations. *Mar. Pollut. Bull.* 108, 242–262. <http://dx.doi.org/10.1016/j.marpolbul.2016.03.071>.
- Valdez Banda, O.A., Hänninen, M., Lappalainen, J., Kujala, P., Goerlandt, F., 2016b. A method for extracting key performance indicators from maritime safety management norms. *WMU J. Marit. Aff.* 15, 237–265. <http://dx.doi.org/10.1007/s13437-015-0095-z>.
- Valdez Banda, O.A., Goerlandt, F., 2017. The design of VTS Finland Safety Intent Specification. Aalto University publication series (Science + Technology).
- Valdez Banda, O.A., Goerlandt, F., Salokannel, J., 2018. A process for validation of safety management systems. To be submitted in Safety Science.
- Wahlström, B., Rollenhagen, C., 2014. Safety management – a multi-level control problem. *Saf. Sci.*, PSAM11 – ESREL 2012 69, 3–17. < <https://doi.org/10.1016/j.ssci.2013.06.002> > .
- van Westrenen, F., Praetorius, G., 2012. Maritime traffic management: a need for central coordination? *Cogn. Technol. Work* 16, 59–70. <http://dx.doi.org/10.1007/s10111-012-0244-5>.