Transportation Research Part A 166 (2022) 369–388

Contents lists available at ScienceDirect

Transportation Research Part A

journal homepage: www.elsevier.com/locate/tra

Safety and security co-analysis in transport systems: Current state and regulatory development

Shiqi Fan, Zaili Yang *

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, Liverpool, UK

ARTICLE INFO

Keywords:
Safety
Security
Transport systems
safety and security co-analysis (SSCA)
Multimodal transport

ABSTRACT

Transportation is sensitive to risk. Given the fast development of digitalisation and automation of transport systems in the past decade, new types of security risks (e.g. cyberattacks) emerge within the context of transport safety research. To enable the integrated analysis of emerging security and classical safety-related risks in a holistic manner, safety and security co-analysis (SSCA) is highly demanded for accident prevention. SSCA in transport systems will benefit the risk analysis of complex cyber physical transport systems facing challenges from both hazards and threats. However, the nature of hazard and threat-based risks is fundamentally different, which leads to the various difficulties of analysing them on the same plane. They include the use of different risk parameters, the uncertainty levels of the risk input and the methodologies of risk inference. To address such concerns, this study firstly reviews the literature on SSCA and compares the employed methodologies and their applications within the context of transport systems. Taking into account the advantages of both security-driven and safety-oriented methods, a conceptual framework is proposed to imply the insights on SSCA for transportation through both top-down and bottom-up perspectives, followed by a quantitative illustrative case study. Then, the regulatory development and evolution of SSCA in transport in practice is analysed across different transport modes, which configures initiatives' interrelations for a cross-fertilisation purpose. As a result, the findings reveal new research directions for the safety of digitalised and/or autonomous transport vehicles and aid in the formation of future transport safety study agendas.

1. Introduction

Since the terrorist attacks of 9/11, security risk analysis has become a necessity for the world (Hawila and Chirayath, 2018). Safety and security are regarded as general terms in every-one life, however the research on safety and security co-analysis (SSCA) under the same framework is much less compared to the studies from an individual perspective. Safety analysis focuses on hazards while security is more threat driven. Different from a hazard (often described as a physical situation), a threat is defined as an action or potential action that could cause loss of life, or damage to property and/or environment (Yang and Qu, 2016). Because of this fundamental difference, it is more challenging to model security risk using safety analysis techniques, as an action involves uncertainty at a higher level and usually is more affected by external sources (Yang et al., 2009).

SSCA can be defined as the integrated analysis of emerging security and classical safety-related risks in a holistic manner for the prevention of accidents/incidents in complex systems. Because there are few models to balance interrelated safety and security control

* Corresponding author at: James Parsons Building, Byrom Street, Liverpool L3 3AF, UK.
E-mail address: z.yang@ljmu.ac.uk (Z. Yang).

https://doi.org/10.1016/j.tra.2022.11.005

Available online 17 November 2022

Table 1
Terminologies for SSCA.

Term	Definition	References
Accident	"An unplanned event or serious of events leading to death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment".	Ericson (2015)
Incident	"An intentional event or serious of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment".	Ericson (2015)
Loss	"It involves something of value to stakeholders, including the loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders".	Leveson and Thomas (2018)
Hazard	"Any actual or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment, or property; or damage to the environment".	Ericson (2015)
Threat	"This is the person or thing that is vulnerable to injury and/or damage, and it describes the severity of the mishap event. This is the mishap outcome and the expected consequential damage and loss".	Ericson (2015)
Loss scenario	"A loss scenario describes the causal factors that can lead to unsafety control actions and hazards".	Leveson and Thomas (2018)

measures, policymakers usually make an unenviable choice of sacrificing safety for security or vice versa (Branscomb et al., 2012). For example, Rail America's filing (AGR tariff 9000) outline the policy for handling toxic inhalation hazard (TIH) shipments that solely focus on improving safety without essential security measures appropriately involved, because of the contradiction of sustaining both safety and security. Under the policy described by the Surface Transportation Board (STB), the dedicated trains convey TIH cars with shipment approval taking 5 days to be issued. Furthermore, each train has no more than 3 TIH cars and moves at speed under 10 miles per hour to ensure high-level safety. However, from a security perspective, the case exposes a high vulnerability, because the provision of the safety measures easibly causes growing security risks such as a long lead time (5 days) for criminals (incl. terrorists) to prepare for any attack and access the target train at a low speed. It is therefore imperative to develop a new SSCA framework for balancing interrelated safety and security control measures in transport systems. In addition, the high level of data uncertainty for security studies makes it difficult to integrate them with safety data for a comprehensive analysis. The methodology of safety analysis identifies hazards from system perspectives, while the one of security studies extracts failure scenarios with components, which results in the failure of synchronising safety and security. Safety and security risks are separately treated traditionally, cannot be tackled in a holistic way due to the facts that 1) transportation is very sensitive to risks and the safety study concentrates on the hazards and mistakes/errors associated with transport systems, while the security study focuses on the actions to impact (Olojede et al., 2017); 2) the high data uncertainty of security analysis makes the integration of safety and security difficult; 3) the safety model evaluate risks from system to components, while the security model starts with the misuse case and ends up with failure effects; 4) the error-oriented safety studies identify the vulnerability of system and nodes, while the cyber-oriented security studies choose the most vulnerable parts as direct attacks or indirect ones as the intermedia; 5) the demand for SSCA is fast growing in the digital and autonomous transport era. It is even more worrisome given the fast-growing applications of cyber-physical systems in today's digitalisation and automation era. Having said that, both safety and security risks in transport systems share common parameters (e.g. likelihood and consequene severity) for their assessment, which provides a possibity of SSCA.

Events causing security attacks are defined as threats, while those that cause safety problems are called as hazards (Lautieri et al., 2005). Furthermore, "safety risks" derive from unintended mistakes or errors, whereas "security risks" come from deliberate actions to impact (Gromule et al., 2017). It is also argued that "safety risks" are caused by both internal and external factors, while "security risks" mainly result from external sources, possibly with internal aids. Hence "security risks" tend to be more difficult to control and manage (Yang and Qu, 2016). Safety risk assessment without taking into account the possibility of security disruptions would underestimate the risk level of any transport system. Security breaches are perceived as more threatening than safety concerns because that 1) they often cause the larger scale of severity of damage (Coppola and Silvestri, 2020), despite arguably lower frequency of occurrence and 2) compared to safety, the occurrence of security accidents is involved with a high-level uncertainty and often out of the company's control. Despite the high demand and benefits in practice, SSCA research has primarily been conducted separately in the current transport literature, and categorised into three groups: pure security initiating event analysis, pure safety initiating event analysis, and an integrated analysis for either a security or safety initiating event (Hawila and Chirayath, 2018). Furthermore, the developments of SSCA against different transport modes reveal significant difference. It will be beneficial to compare the SSCA developments across different modes for a cross-fertilization purpose.

In the meantime, the use of new advanced technologies and complicated systematic engineering stimulates the study on the

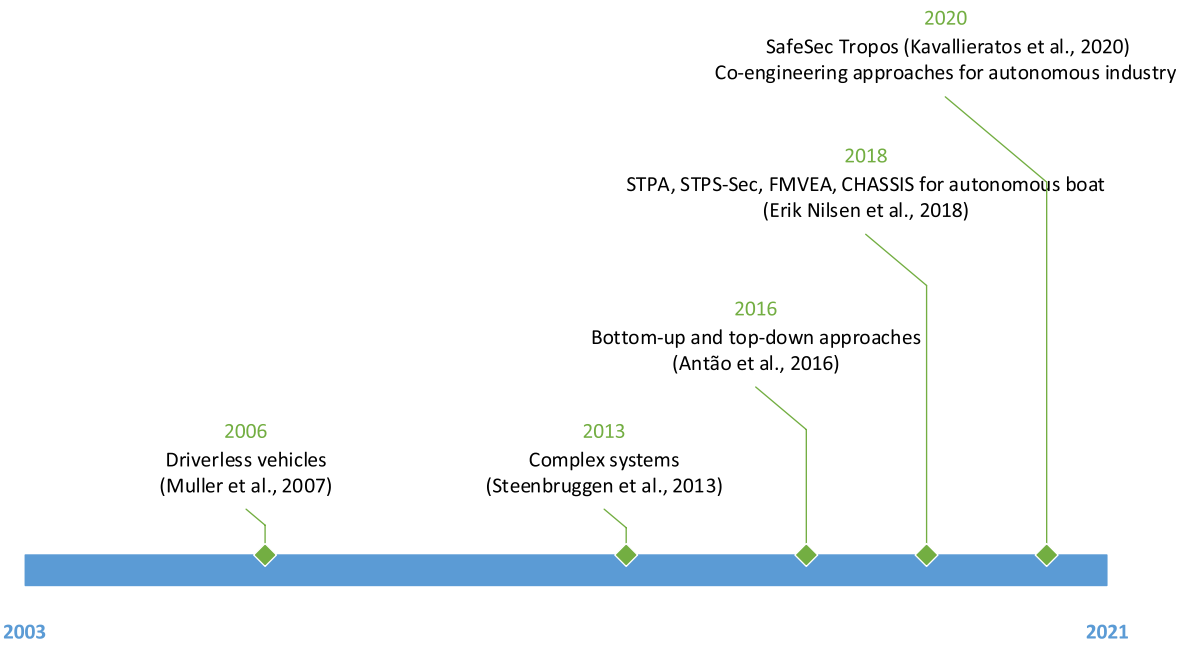

Fig. 1. Milestones of SSCA research.

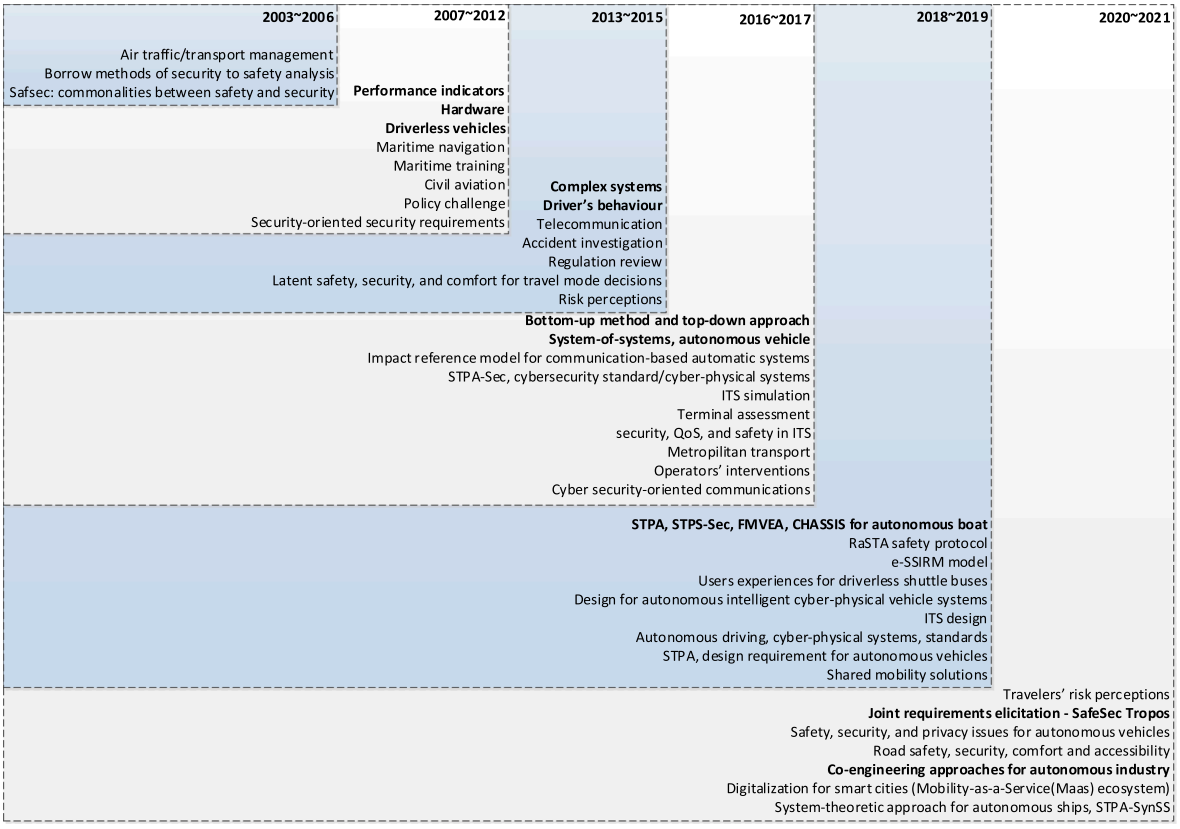

Fig. 2. Evolution of the research themes of SSCA.

feasibility of applying traditional single-dimensional safety assessment approaches to the transport system-of-systems (SoS). Along with the operational complexity of SoS and the demands for the tradeoff with availability and performance (from a safety analysis perspective), the unauthorised access and malicious interruption of systems will compromise the security, resulting in the error-prone decision on the occurrence of accidental consequences. It is evident that such security risks permeate the SoS, however have yet been sufficiently incorporated into the traditional safety assessment methods (Chen et al., 2016). In light of this gap, safety should interact with security to achieve robust and resilient transport systems today and in the future, much more urgent than ever.

Compared to physical security threats (e.g. terrorist and pirate attacks (Jiang and Lu, 2020)), cyber security risks attract increasing attention due to the rising automation systems and/or autonomous vehicles used in transportation (Cheung et al., 2021). From a multimodal transport perspective, the security levels of land transport terminals, airports, and seaports should be remained at the same level (Gromule et al., 2017) because the vulnerability in any part of a whole system could be transmitted and affect the other parts. In other words, the security level of the whole system is equivalent to the part with the highest level of vulnerability. Compared to safety, security in transportation networks possesses a stronger characteristic of risk transmission across different nodes/links. For example, in a global supply chain, if cargo ships at sea are hijacked by terrorist attacks, they can be used as weapons to attack ports or other transport infrastructures through inland waterways and hence cause the failure of the supply chain. The other illustrative example is container transport integrating many different modes, among which the most vulnerable parts will often be chosen for direct attacks or indirect ones as the intermedia (e.g. loads of explosive cargo). The necessity of SSCA in theory and its applications in multimodal transport reveal a new research gap to be addressed with urgency, which lacks theoretical implications in the current literature. Therefore, this paper reviews the current state of SSCA in transport systems and proposes a conceptual SSCA framework by integrating advantages of both security-driven and safety-driven methods. The novelty of this paper lies in the construction of SSCA through both top-down and bottom-up perspectives, followed by a quantitative case study using fuzzy evidential reasoning (FER) to investigate the SSCA of ports. Then the initiative/regulatory analysis is conducted to reveal the current development of safety and security in practice from different transport modes and help consolidate the interrelations among them in regulatory standards. The results aid to analyse and define emerging research topics in transport safety research agenda.

The structure of the paper is organised as follows. Section 2 conducts the literature review on the SSCA research themes. Section 3 draws out the state of the art of the current SSCA, including transport modes, concepts of SSCA, and research methods. A conceptual SSCA framework for transport systems is proposed by comparative analysis of methodologies in Section 4. The regulatory development of SSCA is analysed in Section 5, followed by the conclusions in Section 6.

2. Evolution of SSCA research themes

To define the state of the art of SSCA, a thorough review was conducted, comprising of four steps: (1) online searching, (2) abstract filtering, (3) full-text screening, (4) refining and analysing. Firstly, the online databases selected for this study are the Web of Science and the Scopus databases. Both of them are among the most comprehensive and representative multidisciplinary content searching sources (Lisova et al., 2019). The keywords for the Web of Science searching with a period from 1970 to 2021 were "safety (Topic) and security (Topic) and transport* (Topic)", "safety (Topic) and security (Topic) and road (Topic)", "safety (Topic) and security (Topic) and rail (Topic)", and "safety (Topic) and security (Topic) and maritime (Topic)". After reading and checking abstracts and keywords in this process, we excluded the publications with irrelevant topics. Then, the same searching strings were applied to the Scopus. After filtering out redundant publications and screening full-text, there were 58 relevant papers included in the study.

The remaining academic articles constitute the database for this study. The above publications were further refined and analysed from several perspectives, including transport fields, concepts, research methods, methodologies, associated standards, autonomous topics, and applications. Among these perspectives, transport fields and associated standards imply the past development of SSCA in different transport sectors. Concepts, research methods, and methodologies provide rational clues for the SSCA framework. In addition, autonomous topics and applications show the necessity and tendency of using SSCA in future transport studies. Table 1 presents various terminologies within the scope to help understand relevant theories in the SSCA.

Systematic review can be conducted by different tools (e.g. Citespace) depending on the complication of the search setting. In this case, both traditional searches using keywords and Citespace tool were applied. The results reveal that the traditional method presents the relevant papers better than Citespace, as some important and relevant papers identified manually were skipped from Citespace. It is because that the key words used for the search were derived from not only key words (i.e. Citespace case) but also other parts of the selected papers (e.g. full paper).

Significant milestones of SSCA development since 2003 are shown in Fig. 1. The milestone years are selected based on the following criteria: 1) in the literature, a significant increase of the relevant papers in academics during and after the chosen milestone years (e.g., 2007), or 2) clear and direct supporting evidence from industrial development (i.e. significant technology evolution) (e.g., 2013). The SSCA was applied to driverless vehicles in 2007 (Muller et al., 2007) and complex systems in 2013 (Steenbruggen et al., 2013; Bezzateev et al., 2013; Dong et al., 2013). The proposition of bottom-up and top-down methods in 2016 witnessed the application of SSCA in SoS (Antão et al., 2016). In 2018, more models (e.g. STPA, STPS-*Sec*) had been developed to investigate multi-criteria for the SSCA (Erik Nilsen et al., 2018), followed by co-engineering approaches applied in autonomous industry in 2020 (Török and Pethő, 2020). At the beginning of the SSCA development, as seen in Fig. 2, the co-analysis concentrated on voice communication in air traffic control in the aviation field. Driven by digital signal transmission, the proposed techniques overcame the security issues (poor voice quality with ambiguity during transmission) for better air traffic management (Hering et al., 2003). From 2003 to 2006, the research themes were shifted by incorporating security methods to safety analyses and exploring commonalities between them. Due to the co-existence of safety and security issues in transport systems, an SSCA conceptual work was developed by mainly using security-based techniques to deal with malicious adversaries and assess the systems' security vulnerability (Johnston, 2004). Along with the standard studies on air transport software certification, large collective research projects, such as SafSec, effectively illustrated the necessity and benefits of undertaking a combined analysis and further aided to document a combined argument for SSCA (Lautieri et al., 2005).

From 2007 to 2012, more attention has been paid to safety and security associated key performance indicators (KPIs) and hardware-driven security requirements. Through a series of interviews, workshops, and questionnaires, the KPIs for airport safety and security were developed, revealing that it is critical to enhancing intelligence and information sharing for preventing terrorism and

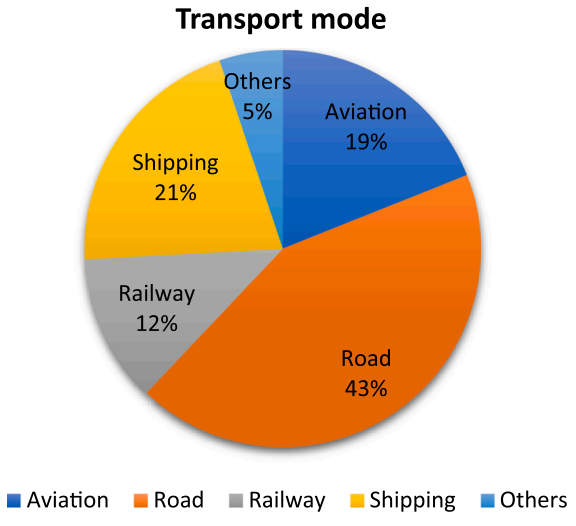

Fig. 3. Numer of SSCA in terms of different transport modes.

crimes at airports (Enoma and Allen, 2007). Furthermore, owing to automation and demands on security information transformation between systems, the security concerns derived from new technologies emerged, including driverless vehicles in road transport (Kubota et al., 2007), civil aviation (Guthrie, 2011), and maritime navigation and training (Urbanski et al., 2008; Ou and Zhu, 2008). With regards to such concerns, the necessity of combining safety and security was further emphasised, as well as the policy challenges for the revolution of security requirements in transport systems (Branscomb et al., 2012). During this period, the solutions to the security problems were revisited using safety techniques, while safety concerns were retreated in security thinking. In addition, the road and maritime transport sectors accelerated their momentum on SSCA studies, in particularly based on the lessons from the aviation sector.

Complex system problems emerged with the system safety theory and risk perceptions in 2013–2015. The SSCA was conducted more holistically for accident investigation, regulation review, and rational decision-making to support traffic planning. Regulatory reviews were undertaken to clarify the responsibility of various authorities and identify their drawbacks for air traffic accidents. It recognised the critical role of combined safety and security analysis for ensuring the robustness of transport systems (Abeyratne, 2014; Fox, 2014). As far as the travel of school children is concerned, road crashes, dislocation and kidnapping were characterised as the main challenges for them (Ipingbemi and Aiworo, 2013). Although the percentage of involved in road crashes or kidnapped was relatively low, the government must prioritise the access needs of school children and improve transport policy addressing their access requirements through SSCA. Concerning travel modes, survey data about the safety, security, and comfort attributes of train stations was collected to show their impacts on mode choice by a marginal change in a fatality index (Daziano and Rizzi, 2015). The travel decision was made based on subjective attributes (safety, security, and comfort) instead of objective attributes such as time and cost. The SSCA measured the impact of safety and security on choice so as to estimate and forecast the travel mode decision. In addition, a public transport study used hierarchical cluster analysis to show that safety and security factors were less relevant for work or education travels than leisure travels (Nordfjaern et al., 2015). It was evident that the decreased intention of using public transport was associated with high perceived probabilities of accidents and security-related risk perceptions through the SSCA (Marquez and Soto, 2021). Hence, transport authorities need to prioritise the development of effective solutions to security issues for public transport. In this period, it is found that more and more SSCA co-existence studies were carried out, in which either safety and security are analysed holistically or they are presented in the same risk-based frameworks.

From 2016 to 2017, researchers started to investigate the methodologies of SSCA using both bottom-up and top-down methods derived from traditional safety models or security frameworks. Further, the concepts of system-of-systems and cyber-physical systems (CPSs) had been proposed due to the development of autonomous vehicles and intelligent technology applications in transport systems. For instance, Antão et al. (2016) conducted a bottom-up approach to generate an indicators inventory with respect to occupational health, safety, and security based on annual sustainability reports of seaports, while a top-down method was conducted based on legislation, regulations, and the feedback from stakeholders in the seaport and shipping industries. In addition, Cooperative Intelligent Transport Systems and CPSs for autonomous vehicles had been investigated and developed to rationalise the designs of vehicles and infrastructures (Chen et al., 2016). Within the context of automotive cybersecurity standards, the applicability of models to analyse high-level safety and security events was discussed, and the challenges of assessing potential safety and security risks at the beginning of a system's development lifecycle were identified (Schmittner et al., 2016).

From 2018 to 2019, the SSCA of autonomous systems grew very fast involving more new models, including Systems Theoretic Process Analysis (STPA), System-Theoretic Process Analysis for Security (STPA-*Sec*), Failure Mode, Vulnerabilities and Effects Analysis (FMVEA), Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS), and Safety and Security Impact Reference Model (SSIRM), etc. Torkildson et al. (2018) conducted an empirical study to compare SSCA methods with the case of an autonomous boat. Although STPA and STPA-*Sec* and CHASSIS methods were time-consuming, but they could identify more hazards in autonomous systems. Moreover, an autonomous shuttle bus study revealed that the subjective perception of security in driverless buses

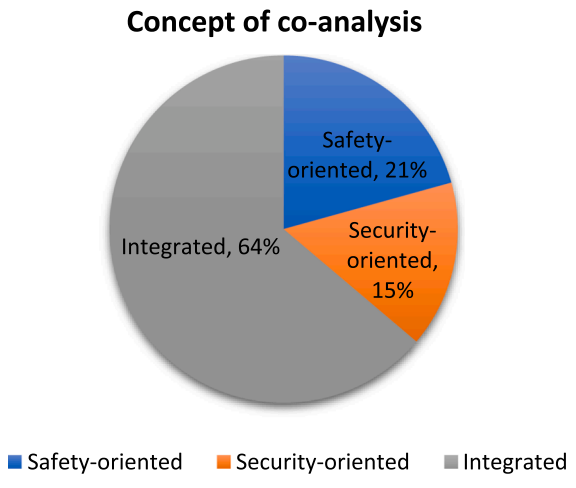

Fig. 4. Concepts of safety and security co-analysis.

varied from conventional buses (Salonen, 2018). A worse sense of in-vehicle security needed to be improved, especially for female passengers. Tokody et al. (2018) used a cyber-security approach to improve the safety and cybersecurity design for an original safety system. There were gradually increasing demands on autonomous intelligent transport systems, triggering more SSCA in the area.

From 2020 to 2021, co-engineering approaches and digitalised-driven SSCA were developed in autonomous systems. Given the security and safety challenges of CPSs, Kavallieratos et al. (2020) proposed a combined method for safety and security engineering for the system design in the lifecycle. Such a method, namely SafeSec Tropos, facilitated the holistic SSCA for autonomous ships and provided documentation regarding the conflicts of the identified safety and security requirements. Regarding the integrated evaluation of safety and security, a scenario-based method was applied to the complex SoS operation processes (Török and Pethő, 2020). From this point of view, future directions of autonomous security were proposed based on safety and security co-engineering. Within this context, maritime automation was enriched by the system-theoretic SSCA. Zhou et al. (2021) developed an STPA-SynSS model to identify SSCA factors and develop mitigation strategies to benefit autonomous ships with design process and shore control centre by addressing both safety and security risks simultaneously.

Although the SSCA has been developed in transport systems, the theoretical implications in multimodal transport remain scanty. To enable the comparison of emerging security and classical safety-related risks in a holistic manner, SSCA in transport systems includes the use of different risk parameters, the uncertainty level of the risk input and the methodologies of risk inference. Most of these methods are not integrated into systematic risk analysis. In addition, there is no methodology to conduct SSCA for autonomous vehicles which have been fast developed in the past decade. To address such concerns, this study, based on the analysis of state of the art on SSCA, proposes a new conceptual SSCA in transportation by investigating the advantages and disadvantages of existing methodologies and their previous applications in different transport modes. The study integrating security-driven and safety-driven methods makes new contributions: 1) top-down and bottom-up methods are integrated based on the review of SSCA in transport systems; 2) a methodology is proposed to optimise system design aiming at digitalised and/or autonomous transport vehicles;3) regulatory evolution is revealed to show the future directions of SSCA in transport.

3. The state-of-the-art of SSCA in transportation

In the current literature, the existing SSCA frameworks used to analyse transportation systems were systematically examined. The transport modes, research concepts of SSCA (i.e., safety-oriented co-analysis, security-oriented co-analysis, and integrated co-analysis), and research methods (e.g., survey, case study, conceptual work, simulation, and others) imply the diversity and flexibility of the relevant research topics.

3.1. Transport modes

SSCA has been applied in different transport modes, including aviation, road, railway, shipping, and others, as shown in Fig. 3. The aviation sector accounts for 19 % of the total studies. It mainly focused on air transport (Kesseler, 2004; Abeyratne, 2012), accident investigation (Abeyratne, 2014; van Asselt, 2018), airport performance (Enoma and Allen, 2007), civil aviation (Guthrie, 2011), air traffic (Hering et al., 2003), aircraft modular systems and applications (Lautieri et al., 2005; Vlissidis et al., 2017). In terms of road transport, it concentrated on vehicles/autonomous vehicles (Sharma et al., 2019; Ben Hamida et al., 2017), buses (Salonen, 2018; Olfindo, 2021), coaches (Gromule et al., 2017), as well as smart cities (Acheampong, 2021), which takes 43 % of the total papers. The railway and shipping sectors occupy the same percentage (i.e. 12 %). Among the railway studies, supply chains (Branscomb et al., 2012), automated control systems (Bezzateev et al., 2013; Pawlik, 2016), and risk perceptions (Coppola and Silvestri, 2020; Coppola

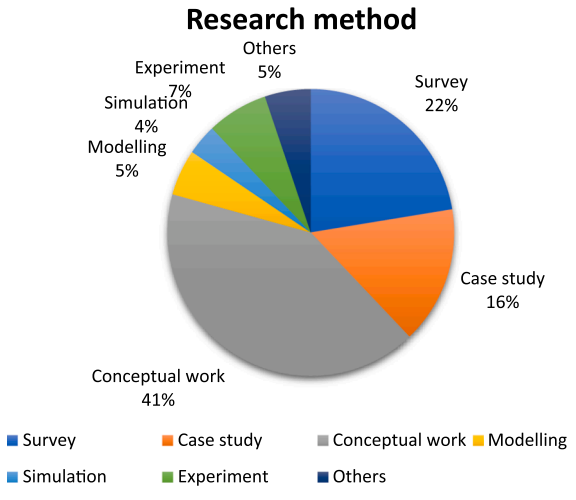

Fig. 5. Research methods for safety and security co-analysis.

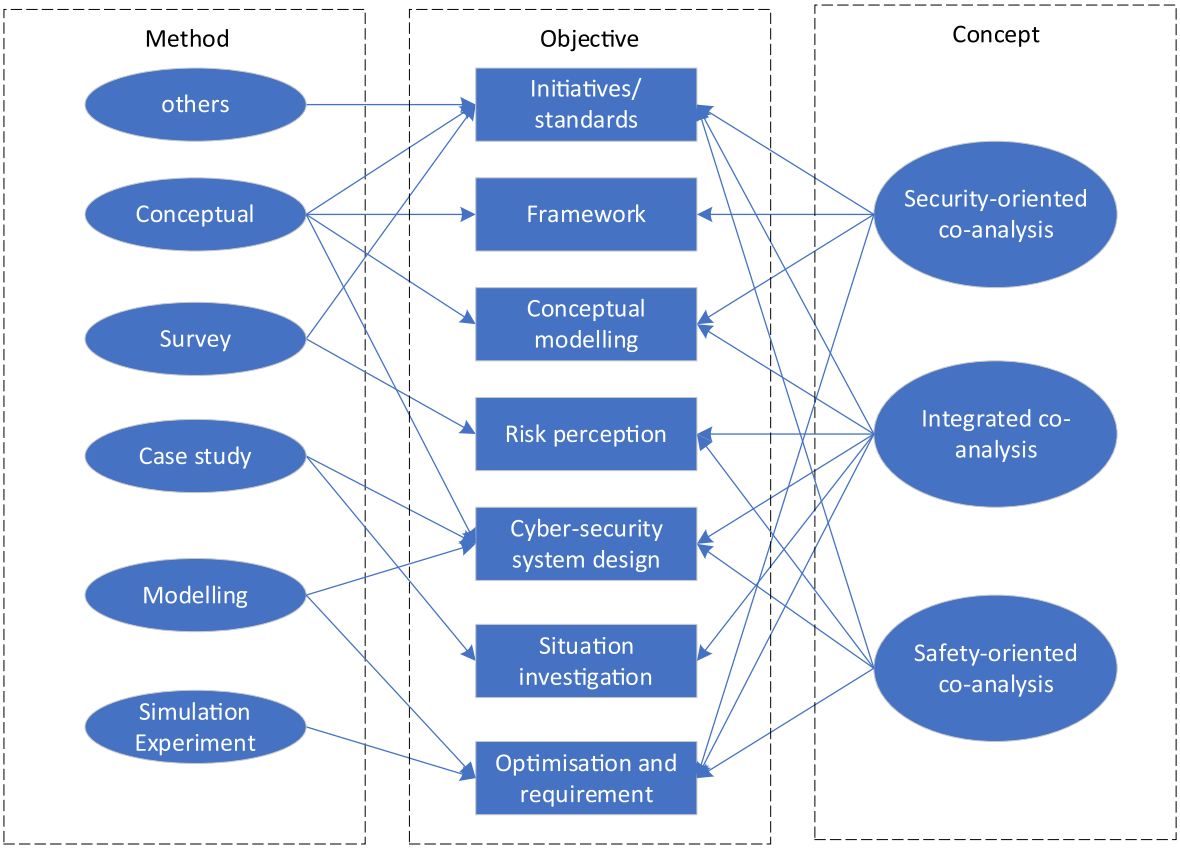

Fig. 6. Current state of SSCA.

and Silvestri, 2021) were heavily investigated. Concerning the maritime sector, autonomous systems illustrate the SSCA with the development of cyber physical systems in the shipping industry (Kavallieratos et al., 2020; Zhou et al., 2021; Guzman et al., 2020). Further, maritime domain awareness (Ou and Zhu, 2008), maritime education and training (Baldauf et al., 2012; Alam et al., 2021), autonomous ship design and requirement (Bolbot et al., 2021; Dghaym et al., 2021) were explored. Besides, combined transport modes, such as mixed travel modes decision (Daziano and Rizzi, 2015) and perceived risk analysis (Nordfjaern et al., 2015; Marquez and Soto, 2021) were proposed in terms of SSCA. It is evidence that SSCA in autonomous cars and aircrafts is ahead of the other sectors. Given the increasing demands on the multimodal transport of containerised cargoes, the SSCA crossing multi-sectors and comparisons among the methods applied in different transport modes are insightful. However, there are few studies on SSCA of multimodal transport, revealing a new research gap to address.

3.2. *Concepts of SSCA in transportation*

The SSCA in transport systems involves different risk analysis mechanisms, including tackling security issues of safety control, safety problems of security measures, and integrated analysis of complex systems. The co-analysis studies that mainly aimed to solve the safety issues or prioritise the safety in the investigation are defined as safety-oriented co-analysis studies, while those focusing more on security breaches or having a priority on the security of a system are regarded as security-oriented co-analysis studies. Moreover, the study investigating both with the same priority is described as integrated co-analysis. As shown in Fig. 4, there were 21 % of the research on the safety-oriented co-analysis. It solved the safety issues in transport systems (Abeyratne, 2014), established safety-driven security models (Bezzateev et al., 2013), developed safety-oriented standards to improve security levels (Kesseler, 2004), and undertook the safety planning of complex cyber-physical systems (Urbanski et al., 2008). In addition, 15 % of SSCA concentrated on security breaches with the priority. It analysed security control measures and adaptive security mechanisms (Johnston, 2004; Ben Hamida et al., 2017) and the interrelation between security, quality of service and safety awareness (Javed and Hamida, 2017; Ben Hamida et al., 2017). The cyber security-oriented analysis was also discussed via a conceptual model in the road transportation (Tbatou et al., 2017). However, most co-analysis works were integrated assessments on safety and security simultaneously, accounting for 64 %. Among them, some first identified safety and security issues separately, and then concluded their synthesised indicators (Antão et al., 2016; Alam et al., 2021) or proposed mitigation strategies (Branscomb et al., 2012) on the same plate. In this way, the results were combined in terms of safety and security perspectives (Olojede et al., 2017; Salonen, 2018). The others investigated SSCA

in an integrated framework (Urbanski et al., 2008) and utilised a system-theoretic approach to undertaking the SSCA of autonomous systems (Zhou et al., 2021).

3.3. Research methods of SSCA in transportation

Given the necessity of integrating safety and security has been emphasised, research methods developed from a single perspective (i.e. safety or security) will not be applicable for their co-analysis. The research methods applied in SSCA were divided into qualitative methods, (including case study and conceptual work) and quantitative methods, (e.g. survey, modelling, experiment, and simulation). Approximately 66 % of the co-analysis works in transportation systems were qualitative and 34 % quantitative.

As shown in Fig. 5, 41 % of the studies conducted conceptual works, which were rather broad, including conceptual analysis of definitions, initiatives development, theoretical frameworks, and conceptual modelling of safety and security issues. For instance, Török and Pethő (2020) introduced safety and security co-engineering approaches to evaluate the scenario-based safety and security in SoS. Urbanski et al. (2008) investigated the adaption of traditional maritime safety systems to a new circumstance regarding SSCA. 22 % conducted an empirical survey to collect data through questionnaires and interviews. For instance, a survey identified the risk perceptions for passengers in various circumstances to foster mental models concerning safety and security (Salonen, 2018). In addition, Olojede et al. (2017) collected 300 questionnaires to confiture urban transport planning, in which safety and security issues were first analysed separately and then the results were synthesised together to generate policy implications and solutions to both safety and security. In order to establish an in-depth investigation of a particular situation or community, the case study method was used for empirical research, accounting for 16 % of the total work. At the design stage of its lifecycle, a cyber-enabled ship was regarded as a case to illustrate the security and safety challenges in interconnected sub-systems (Kavallieratos et al., 2020). Moreover, the modelling was applied to explain and demonstrate the SSCA, accounting for 5 %. This method was utilised to identify the security-realted hazards in the safety issues (Bezzateev et al., 2013), evaluate automotive cybersecurity standards (Schmittner et al., 2016), and generate system design requirements (Sharma et al., 2019) for autonomous transport systems. The simulation and experiment, which accounted for 4 % and 7 % respectively, were used for system performance optimisation (Ben Hamida et al., 2017) and technology revolution (Mansor et al., 2019). The other method was the review of initiatives, which encompassed 5 % of the total work (Fox, 2014; Guthrie, 2011).

The current security-driven and safety-driven SSCA in transportation involved both qualitative and quantitative methods, as shown in Fig. 6. It included initiatives review, framework study, modelling, risk perception, cyber-security system design, accident investigation, and system requirements.

For example, a cyber security system was designed using qualitative conceptual methods and quantitative modelling, driven by safety-oriented and integrated co-analysis. In addition, the objective of conceptual modelling for autonomous systems was achieved by security-oriented and integrated co-analysis using qualitative methods. It is clearly evident that transport systems were investigated through very diversified SSCA methods and from different perspectives. It is helpful when the safety and security of a multimodal transport supply chain are concerned. The developed pathway of SSCA demonstrates the reality of integrating safety and security issues in transport modes. In contrast, the undeveloped pathway implies the possibility of further research to be explored. Therefore, it is highly demanded to propose a new SSCA framework aiming at transport systems by integrating advantages of security-driven approach and safety-driven method in a multimodal transport system.

4. A conceptual SSCA framework for transport systems

Traditionally there are many qualitative methods used for the SSCA of transport systems. For example, standard/regulatory reviews, a series of interviews, workshops, secondary data research, and purification from the internet and other social media have been presented as effective ways to investigate the integration of safety and security. However, the SSCA of autonomous systems, including drones, driverless cars, and autonomous ships, have been fast developed in the past decade. Under this circumstance, the demand for such systems to be independent of human operators is raised with system models. Several models and quantitative methods have been

Table 2
Analysis of SSCA methodologies.

Methods	Examples	Basic characteristics	Application cases
General approach	Life cycle model	Prefer safety requirements if security negatively impacts safety.	Pre-design stage of automation and control system" (Novak et al., 2007).
	FMVEA	The safety analysis flow chart includes security in the analysis.	Identify the failure and threat modes separately but assess their effects overall (Schmittner et al., 2014a).
Model-based graphical method	CHASSIS	Include the process of using misuse case (MUC) and misuse sequence diagram (MUSD) for unified safety and security assessment.	Perform the tradeoffs between conflicting safety and security mitigations (Raspotnig et al., 2012).
	Bayesian belief network (BBN)	Establish the network of risk factors on safety and security of systems.	Measur the impacts of interrelationships between safety and security on each other and system reliability (Kornecki et al., 2013).
Model-based non-graphic method	STPA/ STPA-*Sec*	A top-down approach derived from the system theoretic accident model and processes (STAMP) causality model, and it is extended for STPA-*sec* to both safety and security.	Identify constraints on unsecured control actions that expose the system to unsafe circumstances when it is subjected to disturbances (Young and Leveson, 2013).

applied to generate new safety and security analysis mechanisms. The priority of safety and security in such systems needs to be well balanced depending on different risk scenarios. Section 4.1 presents the SSCA methodologies and their applications. Then, three different types of methods in transport systems are illustrated and compared in Section 4.2, which implies how to choose the SSCA methodology to solve the safety and security problems. In terms of the comparative analysis and applications of SSCA methods, a new SSCA framework is proposed in Section 4.3 by integrating the advantages of the above methods in Section 4.2. The newly proposed SSCA framework is illustrated by a quantitative case study on seaports in Section 4.4.

4.1. SSCA methodologies

The current state of SSCA shows the advantages of integrating perspectives to achieve various objectives in the transport system (see Fig. 5). However, the disadvantages of SSCA should also be concerned, focusing on the potential hidden requirement conflicts it aims to resolve (Potoglou et al., 2010). A unified approach might reduce the understanding of the systems and prevent a thorough analysis of either property if ignoring the requirement conflicts. Therefore, it is critical for any viable co-analysis method to examine the dependency and mutual interaction between safety and security to address its possible drawbacks. The safety and security co-analysis methods in the current literature are classified into three categories (Kriaa et al., 2015), as shown in Table 2.

4.2. Comparative analysis of SSCA methods in transport systems

There are various SSCA methods in transport systems. Comparative analysis of their advantages and applications provides useful insights for the deleopment of a new SSCA framework in Section 4.3.

Within the defined categories in Table 2, three different types of methods are observed in transport systems. The first type refers to standard/regulatory reviews, interviews, and workshops, which were conducted to develop the KPIs for safety and security. It has been applied in aviation (Kesseler, 2004; Enoma and Allen, 2007; Guthrie, 2011), personal transit on buses (Muller et al., 2007), and incident management in road transport (Steenbruggen et al., 2013). This method was used to define safety and security requirements regarding transport accidents, transport processes, and driving manoeuvres, and hence could aid to analyse the attributes' interdependencies and develop advanced technologies into the field. Aiming at dealing with the situation with limited data, this method enables the conceptual modelling and framework development for SSCA. However, lacking objective data to support analysis results implies that the above methods need to be complemented with other approaches to develop the risk control of systems.

The second type is the survey-based method. Bezzateev et al. (2013) found no concerted approach to analyse the safety and security of complex systems by basic safety and security standards. The study developed a security module to identify security hazards through standard fault tree analysis. Ipingbemi and Aiworo (2013) used descriptive and inferential statistics to analyse the data collected from questionnaires, and to generate travel characteristics. Nordfjaern et al. (2015) surveyed and examined the SSCA factors related to the intentions of people using public transport. The risk perception regarding safety and security was measured. Besides descriptive statistics and t-tests, hierarchical cluster analysis was conducted to identify cluster-solutions of travel mode users. The results showed that safety and security factors were more relevant for leisure travels. In addition, a Relative Importance Index (RII) method was used to measure either their relative importance or their frequency (Olojede et al., 2017). A Relative Safety Index (RSI) was created to assess residents' perception on the RSI of a chosen transport mode, while the Relative Security Index (RSeI) assessed relative security index.

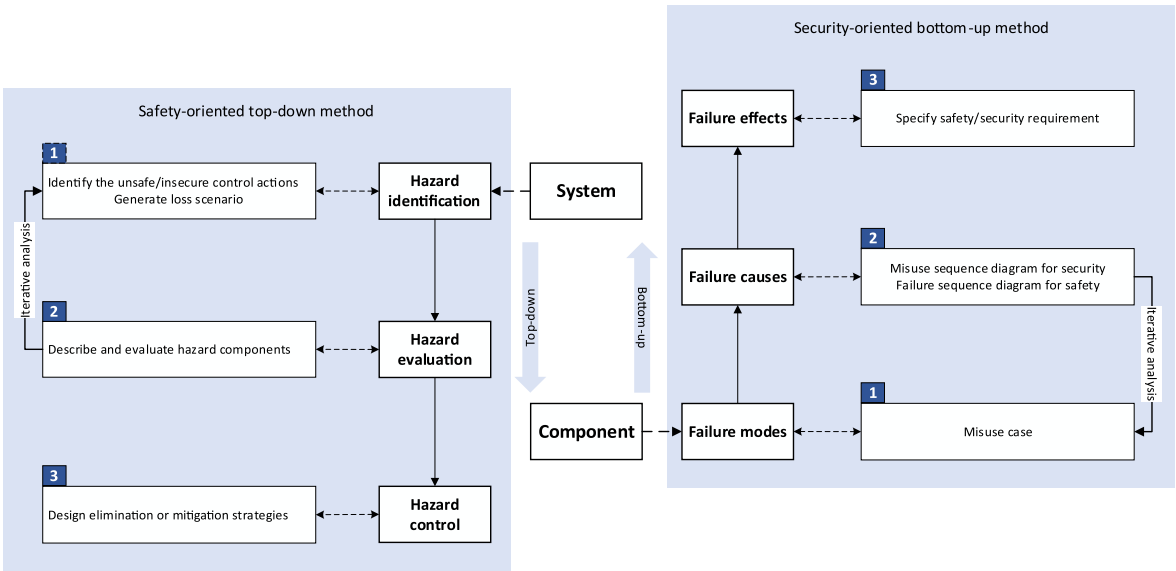

Fig. 7. The new SSCA framework in transport systems.

In addition, learning-objective oriented maritime training was developed to design scenarios for the education, as an enhanced approach rather than an event-driven approach (Baldauf et al., 2012). It illustrated an idea similar to STPA, which generated loss scenarios for security analysis (Zhou et al., 2021). This type of method integrates qualitative and quantitative data for the SSCA in the transport system. Both safety-driven and security-driven approaches can be utilised to conclude insightful findings, which are applicable for the complex system that does not have relevant safety and security standards. Besides, the generation of loss scenarios using a survey-based method makes it possible to apply a security-driven method to solve the breaches in a transport system.

The third category is the model-based method. An SSIRM model subdivided a system into safety and security parts. It has been applied to a railway management system (Pawlik, 2016), in which the safety and security hazards were separately grouped with regard to different functions and illustrated based on the characteristics of situations protected against different cases. Safety hazards included improper preparation, overpassing distance limit, overspeeding, and electrical hazards, while security ones were vandalism, terrorism, passenger health support, natural disaster. It further covered cybersecurity aspects that should be taken into account based on communication between track-side and onboard equipment (Pawlik, 2018). FMVEA (Schmittner et al., 2014b) was derived from the Failure Mode and Effect Analysis (FMEA) method and further developed on the basis of a three-level Data Flow Diagram (DFD) with security analysis. This method simulated the system and identified the failures and threat modes of each component. In terms of failure modes, it covered the safety aspect by demonstrating how the component could potentially fail. With regard to the threat modes, it covered the security aspect by describing how the component could probably be misused. FMVEA (Schmittner et al., 2014b) was applied to the SSCA for cyber-physical systems, i.e., intelligent and cooperative vehicles, regarding the attack possibilities and failure scenarios. Also, it was used to analyse attacks based on the embedded computer in the autonomous boat, Revolt (Torkildson et al., 2018). It included qualitative safety and security analysis, such as component, failure mode, threat mode, failure effect, threat effect, system status, system effect, as well as quantitative analysis, such as severity, system susceptibility, treat properties, attack/failure probabilities and risks.

In addition, CHASSIS (Raspotnig et al., 2012) illustrated a process of using Misuse Case (MUC) and Misuse Sequence Diagram (MUSD) for unified safety and security assessment. MUC combined with MUSD were used for security analysis, while MUC integrated with Failure Sequence Diagram (FSD) were used for safety assessment. The first stage of the CHASSIS process was to create use cases and sequence diagrams based on operational and environmental descriptions of a system for eliciting functional requirements. In the second stage, MUC diagrams were created using hazard and operability study (HAZOP) guidewords for the use cases, and then described in textual MUC templates. Then, FSDs and MUSDs were utilised to refine the hazard scenarios defined in the templates. In the third stage, HAZOP tables were prepared after the textual misuse cases were completed, and corresponding safety or security requirements were specified. Torkildson et al. (2018) utilised this method in the case of "operating and monitoring Revolt remotely through the Revolt Intelligent System". The findings aided to identify and draw safety and security misuse case diagrams, respectively. Further, Raspotnig et al. (2012) applied this method to determine the common countermeasures and solve the SSCA issues and those in conflict dealing with problems for air traffic management.

The STPA is a top-down safety hazard analysis method developed to cope with the increasing cyber-physical systems with advanced technologies. It has been developed and extended into several models to support SSCA of complex transport systems. To begin with, STPA was developed as STPA-*Sec* to be applied for safety–critical CPS in vehicles (Schmittner et al., 2016). In such interconnected systems, hazards were treated as a control problem to be solved for security analysis, which pointed out some overlaps between fault prevention and constraints of a system on taking safe actions. Therefore, STPA-*Sec* does not align entirely with current safety and security standards and needs to extend complementary methods when developing a system in a standard-conform way. It was also highlighted in ISO26262 with the requirement to use top-down and bottom-up analysis methods. Given the unacceptable losses/accidents and safety constraints, the STPA and STPA-*Sec* analysis methods identified unsafe control actions (UCA) through the ship's network structure and control structure documents (Torkildson et al., 2018). Then, the potential causal factors leading to the UCA were identified, followed by STPA-*Sec* analysis. Sharma et al. (2019) utilised the STPA to generate system design requirements for an Autonomous Emergency Braking system and provided a structural approach to scenario analysis. It addressed the research gap of

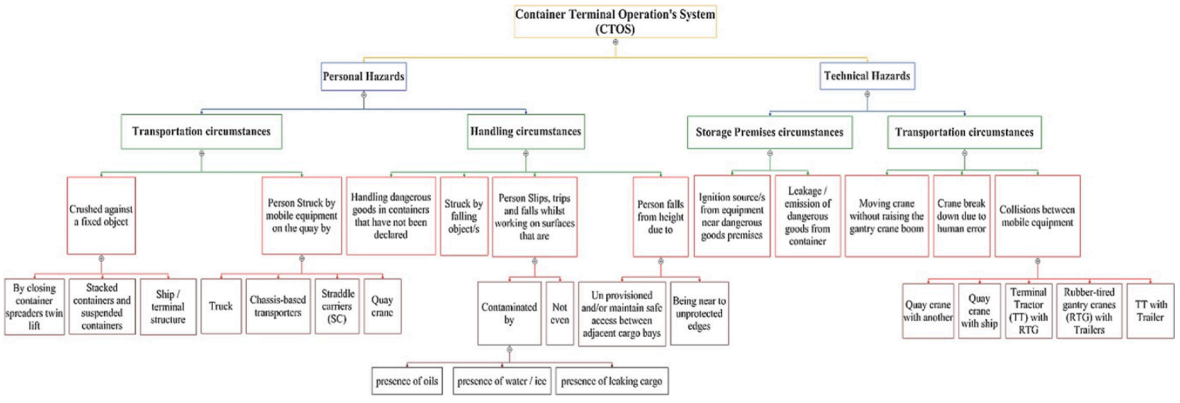

Fig. 8. Hierarchy for the HEs in terminal operations ().
Source: Alyami et al. (2019)

existing designs in the autonomous field and the need for the STPA to be integrated with the ISO standards to produce more efficient outcomes. Kavallieratos et al. (2020) integrated SafeSec Tropos and STPA to conduct a case study on the Cyber-Enabled Ship (C-ES), which revealed the three most vulnerable onboard systems, i.e., the AIS, the ECDIS, and the GMDSS, and identified their relevant safety and security requirements. Zhou et al. (2021) synthesised safety and security by proposing the STPA-SynSS method, which benefited the hazard tracking and dynamic management in terms of system design.

The above model-based methods illustrate advantages of integration of qualitative and quantitative approaches aiming at complex systems in different transport sectors. Moreover, due to various risk analysis mechanisms in models, these methods can be chosen and utilised to support the new SSCA framework in Section 4.3. In the meantime, it is noteworthy that the above analysed methods are those appearing in SSCA analysis based on the core journal papers from WoS and Scoups. Some risk analysis methods such as a functional resonance analysis method (FRAM) (Patriarca et al., 2020) have yet been popularised in SSCA despite their development in individual safety or security research.

4.3. A new SSCA framework

Based on comparative analysis of existing methodologies, a new SSCA framework in transport systems is proposed by integrating both security-driven and safety-driven methods. There are two perspectives on SSCA for complex systems: the safety-oriented top-down method and the security-oriented bottom-up approach, which can solve the SSCA issues separately and/or holistically, depending on the risk control requirements in scenarios. Fig. 7 illustrates the flowchart of the new framework.

Complex systems (e.g. cyber-security systems, autonomous systems, SoS) consist of sub-systems and components. The top-down safety methods are used first to break down a system into components. In such a process, the hazards can be identified from system to component levels. Then security-driven bottom-up approaches can be used to analyse the threats and security risks from component to system level. The rotation goes on until all the hazards and threats are identified and evaluated. Then control measures can be developed and selected based on their effectiveness to both the hazards and threats of high risks. At the same time, safety and security requirements can be obtained based on the failure effects, as shown in Fig. 7.

For example, the SSCA of a complex system can be first conducted using the safety-driven top-down methods, i.e., hazard identification, hazard evaluation, and hazard control. The first step of such a top-down method is to identify unsafe and insecure control actions from a systematic perspective, generating the loss scenarios. The second step describes and evaluates hazard components at the system's bottom. This process can be iteratively analysed to generate more unsafety/insecure evaluations. Such top-down methods can

Table 3
Hierarchy of KSPIs ().

Code	Key security performance indicators (KSPIs)
S	Port facility security level
S-*P*1	*Access control*
S-*P*1-I1	Identify and prevent unauthorized entry to ship/port facility and its restricted areas
S-*P*1-I2	Identify and prevent unauthorized substances introduced into ship/restricted areas of port facility and its restricted areas
S-*P*1-I3	Control activities within the restricted areas
S-*P*1-*I*4	Clearly identify the restricted areas within port facility
S-*P*1-I5	Identification of port personnel, transport workers and visitors
S-*P*2	*Awareness*
S-*P*2-I1	Professional training of security personnel
S-*P*2-I2	Periodic drills and exercises
S-*P*2-I3	Periodic review of security responsibilities and procedures
S-*P*2-*I*4	Periodic inspection to facility so as to ensure that security equipment is properly operated, tested, calibrated and maintained
S-*P*3	*Documentation*
S-*P*3-I1	Periodic review and update of PFSP and other security-related documents
S-*P*3-I2	Prevent unauthorized access, disclosure, amendment and destruction of PFSP and other security-related documents
S-*P*3-I3	Report and maintain records occurrences which threaten the security of port facility
S-*P*4	*Handling of cargoes*
S-*P*4-I1	Supervision of the secure handling cargoes/baggage
S-*P*4-I2	Prevent tampering of cargoes
S-*P*4-I3	Prevent non-carriage entering and storing within storage areas
S-*P*4-*I*4	Routine inspection of cargoes, transport units and storage areas
S-*P*4-I5	Supervision of the secure handling of unaccompanied baggage
S-P5	*Information and interface*
S-P5-I1	Gather and assess information related to security threats
S-P5-I2	Communicate and exchange of information between contracting governments (including the share of best practices)
S-P5-I3	Communicate and exchange of information between designated authorities, facility operators and other security-related institutions
S-*P*6	*Ship/port interface*
S-*P*6-I1	Respond to security threats/breaches of security of port facility or ship/port interface
S-*P*6-I2	Maintain critical operations of port facility or ship/port interface
S-*P*6-I3	Interface with ship security initiatives
S-*P*6-*I*4	Facilitate shore leave for ship personnel
S-*P*6-I5	Facilitate access of visitors to ship, including their identities

Source: Yang et al. (2014)

be supported by models such as STPA, STPA-*Sec*, and STPA-SynSS (explained and described in Section 4.2). After identifying and evaluating components, the co-analysis can be done with the security-driven bottom-up methods, i.e., analysing failure modes, failure causes, and failure effects. This bottom-up approach begins with misuse cases from the component perspective, eliciting the safety and security failure modes. Then misuse sequence diagrams are drawn out to illustrate the security issues. At the same time, failure sequence diagrams are created to represent safety issues. The failure causes explain the failure mode of the transport system, as well as further interact with other failure modes. Such bottom-up analysis can be complemented by several models, e.g., FMVEA, CHASSIS, and HAZOP. At last, the design elimination or mitigation strategy can be developed to control the SSCA in the system. System failure effects are analysed to specify safety and security requirements. Therefore, the proposed framework embraces the key elements and procedures of conducting SSCA, eliminating the barriers in the safety and security analysis combination. The methodology integrates top-down and bottom-up methods to conduct the SSCA in CPSs and SoS. From these perspectives, the hybrid framework provides insights for designing and evaluating autonomous transports.

4.4. A quantitative real case analysis

The new SSCA framework in Section 4.3 is further illustrated within the context of a real case of seaport SSCA in this section. It focuses on a solution to the integrity of safety and security risk analysis results holistically in a quantitative manner.

Alyami et al. (2014) revealed that a high level of uncertainty in data exists in port safety analysis, for which novel flexible risk approaches are needed. Among the most widely applied methods in port safety analysis is Fuzzy Evidential Reasoning (FER) and its extension supplemented by other uncertainty methods such as Bayesian networks (BN) (Alyami et al., 2019; John et al., 2014). In the FER method, fuzzy logic is used to evaluate the risk parameters (e.g. occurrence likelihood and consequence severity), while evidential reasoning aids to locate all the identified hazards in a hierarchy rationally. Following the safety-oriented top-down method in Fig. 7, the most influential 24 hazardous events (HEs) were identified in Step 1 by literature review, accident report investigation, port safety regulations and brain storming in Alyami et al. (2014). The 24 HEs were then positioned against the components in port operational systems in Step 2 (see Fig. 8) for their evaluation using FMEA and BN. The evaluation result of each of 24 HEs was obtained and then synthesised using the ER approach to obtain the overall safety level of the investigated terminal or port. The synthesised result is

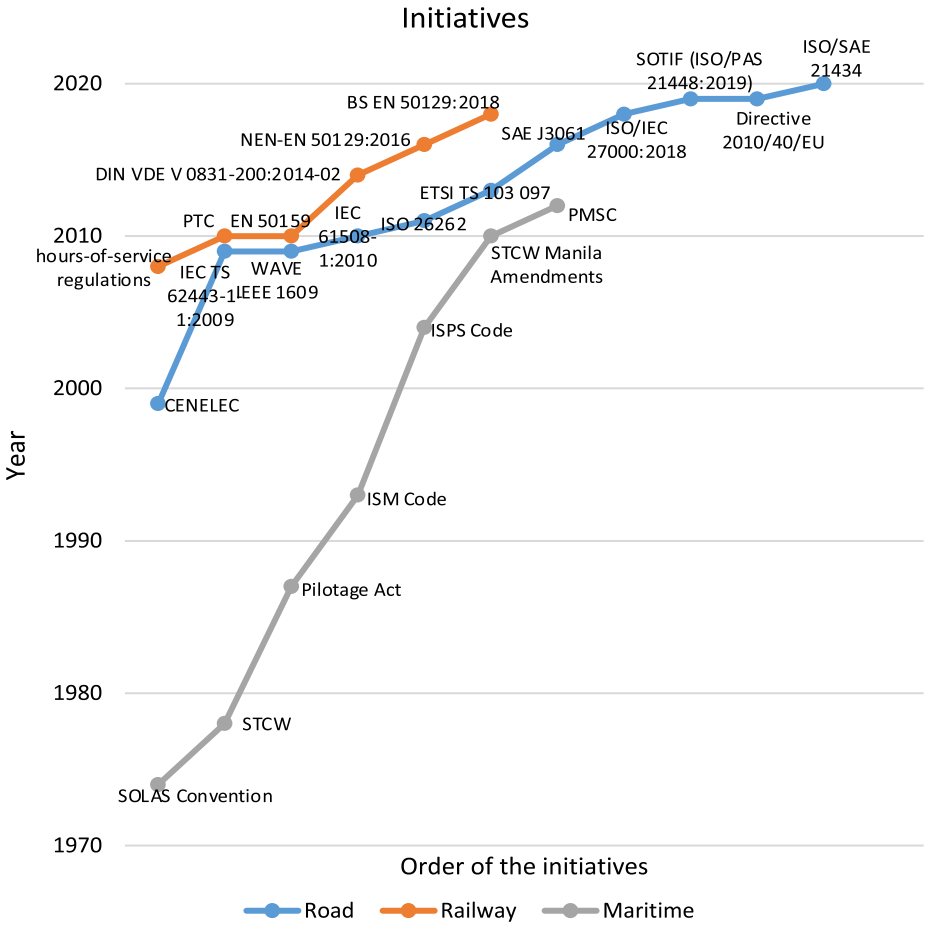

Fig. 9. The initiatives applied to SSCA.

expressed by linguistics terms (e.g. High, Mediem and Low) with a belief degree structure (Alyami et al., 2019), which can be further combined with the security analysis in the same terminal or port when using the same FER method. The HEs of the high-level risks could then be controlled by the measures developed against the relevant HE in Step 1 and the features of component(s) in Step 2 (Alyami et al., 2022).

Very different from the safety analysis, seaport security analysis often starts with attacking modes identification against selected systems' vulnerable components (Yang et al., 2009; Yang et al., 2013; Yang et al., 2014). In other words, in port security analysis, the pair of attack modes (T) and vulnerable components (V) are frequently analysed simultaneously (Yang et al., 2013). The process follows the security-oriented bottom-up mechanism in Fig. 7, including the attack mode analysis and the components being affected by an identified attack mode in Step 1, the root causes contributing to the *T*-V pair in Step 2, and then security risk/effect evaluation in Step 3. For instance, Yang et al. (2005) investigated all the *T*-V pairs of terrorists using possible attack modes (e.g. bombing or hijacked ships for suicide attacks) on different components of a container terminal (e.g. channel and gates). A preliminary screening process was conducted to understand the *T*-V pairs of high risks using a modified risk matrix (Yang et al., 2013). Next, all the key security performance indicators (KSPIs) influencing the high risk *T*-V pairs were generated using the International Ship and Port Facilities Security Code (ISPS) to reveal the failure causes. Such KSPIs (see Table 3) were then evaluated using FER to obtain their failure risk/effect individually at the cause level or jointly for the security levels of the investigated components or the overall terminal system by synthesising the individual results using the FER approach (Yang et al., 2014). The security results at the cause, component and system levels are all expressed by linguistics terms (e.g. High, Medium and Low) with a belief structure. Finally, because both safety and security analysis results are described on the same plane, they can be further combined to generate a single SSCA value to show the risk criticality of an investigated transport system facing all the different types of safety hazards and security threats.

The above demonstrates the detailed integrity of safety and security analysis within the context of seaports using the proposed SSCA framework, including all the detailed mathematical modelling works in each cited reference. To further illustrate how the safety and security results can be combined quantitatively, the ER algorithm as the primary supporting method to realise the above case study, is first provided in the following section, followed by the real numerical integrity of the synthesis of seaport safety and security risk results.

The ER approach (Yang et al., 2009) is further introduced to synthesize the safety and security risk results in seaports. Firstly, the belief degree $\beta_{j,k}$ assigned to the linguistic grades (e.g. High, Medium, Low) are transformed into basic probability masses $m_{D,k}$, which consists of two parts, as shown in Eqs. (1) – (5). The first part is unassigned probability mass derived from the relative importance of the safety risk or security risk results ($\overline{m}_{D,k}$), and the other part is unassigned probability mass generated by the incompleteness of the belief degree ($\widetilde{m}_{D,k}$).

$$m_{j,k} = \omega_k \beta_{j,k} \; j = 1, \cdots, N \tag{1}$$

$$m_{D,k} = 1 - \sum_{j=1}^{N} m_{j,k} = 1 - \omega_k \sum_{j=1}^{N} \beta_{j,k} \tag{2}$$

$$\overline{m}_{D,k} = 1 - \omega_k \tag{3}$$

$$\widetilde{m}_{D,k} = \omega_k \left(1 - \sum_{j=1}^{N} \beta_{j,k}\right) \tag{4}$$

$$m_{D,k} = \overline{m}_{D,k} + \widetilde{m}_{D,k} \tag{5}$$

where R_k means different rules, D is the consequence, ω_k is activation weight of R_k, $m_{j,k}$ represents individual belief degree of R_k belongs to the consequence D, $m_{D,k}$ is the probability mass of R_k.

Then, generate the combined degree of belief of each possible D_j in D by synthesizing both safety and security risk results. Define that $m_{j,I(k)}$ is the combined belief degree in D_j by synthesizing both risk results, and $m_{D,I(k)}$ is the rest belief degree unassigned to any D_j. Let $m_{j,I(1)} = m_{j,1}$ and $m_{D,I(1)} = m_{D,1}$. The overall combined belief degree β_j of D_j is generated by Eqs. (6) – (12).

$$\{D_j\} : m_{j,I(k+1)} = K_{I(k+1)} \times \left(m_{j,I(k)} m_{j,(k+1)} + m_{j,I(k)} m_{D,(k+1)} + m_{D,I(k)} m_{j,(k+1)}\right) \tag{6}$$

$$m_{D,I(k)} = \overline{m}_{D,I(k)} + \widetilde{m}_{D,I(k)} \quad k = 1, \cdots, L \tag{7}$$

$$\{D\} : \widetilde{m}_{D,I(k+1)} = K_{I(k+1)} \times \left(\widetilde{m}_{D,I(k)} \widetilde{m}_{D,(k+1)} + \widetilde{m}_{D,I(k)} \overline{m}_{D,(k+1)} + \overline{m}_{D,I(k)} \widetilde{m}_{D,(k+1)}\right) \tag{8}$$

$$\overline{m}_{D,I(k+1)} = K_{I(k+1)} \times \left(\overline{m}_{D,I(k)} \overline{m}_{D,(k+1)}\right) \tag{9}$$

$$K_{I(k+1)} = \left[1 - \sum_{j=1}^{N} \sum_{\substack{r=1 \\ r \neq j}}^{N} m_{j,I(k)} m_{r,(k+1)}\right]^{-1}, \; k = 1, \cdots, L-1 \tag{10}$$

$$\{D_j\}: \beta_j = m_{j,I(L)}/1 - \overline{m}_{D,I(L)}, j = 1, \cdots, N \tag{11}$$

$$\{D_j\}: \beta_D = \widetilde{m}_{D,I(L)}/1 - \overline{m}_{D,I(L)} \tag{12}$$

where β_j describes the assigned belief degrees to any D_j, β_D describes the remaining unassigned belief degrees to any D_j. The final output calculated by synthesizing both risks is displayed as Eqs. (13).

$$S(A^*) = \{(D_j, \beta_j), j = 1, \cdots, N\} \tag{13}$$

The synthesised safety and security risk result has been obtained until this step. The k in the above equations should be defined as a value of 2 regarding the safety and security risk results. The reason to keep the generic k expression is that the ER approach can be applied to synthesise the safety and security risk results of an overall seaport system and/or of one or multiple components relating to the same sub-systems. For instance, in Alyami et al. (2019), the risk of one HE "HE.6 Crane break down due to human error" has been evaluated as (71 % High, 5.5 % Medium, and 23.5 % Low), where raw data was collected by questionnaire to collect the failure input information from experienced safety officers/port managers (Alyami et al., 2014). In Yang et al. (2014), through the interview, the security risk of a crane in port being attacked by terrorists in three modes (i.e. container bombs, missile attacks and use ship for suicide attacks) is evaluated as (79.1 % High, 17.1 % Medium and 0 % Low, with 3.8 % Unknown). The study reviewed the PFSA practice by five international ports covering four continents (Asia, Europe, North America and Oceania). Given the highly sensitive nature of security data and information, the detailed description of the five ports is kept confidential. The detailed calculation and evaluation of the investigated port against each indicator are documented in Yang et al. (2014). Assuming the two results refer to the same seaport, they can be synthesised using the above ER method (i.e. Eqs (1–13) to have an SSCA value of (80.9 % High, 9.1 % Medium and 9.35 % Low, with 1.46 % Unknown) when safety and security risks are assigned the same weight. This result can be further processed to obtain a crisp value for ranking or control purposes.

5. Regulatory developments of SSCA

Through the comprehensive review of the SSCA, this section describes the SSCA's regulatory evolution involving different transport modes from 1974 to 2020, as seen in Fig. 8. It consolidates the SSCA regulatory development across different transport modes and configures their interrelations for a cross-fertilisation purpose.

In Fig. 9, the middle line illustrates the initiatives released for road transport. In the beginning, CENELEC was released in 1999 to identify safety methods for system components to ensure safety and treat hazardous events. With the development of autonomous technology in road transport, IEC TS 62443–1-1:2009 is published for the technical reference to define the terminology, concepts and models for the Industrial Automation and Control Systems (IACS) security in 2009. Since then, more regulations have introduced security in safety guides. In 2009, IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) defines the characteristics of high speed (up to 27 Mb/s) short-range (up to 1000 m) low latency wireless communications in the vehicular environment regarding security mechanisms and physical access. In addition, ISO 26262, defined by the International Organization for Standardization in 2011, is titled "Road vehicles – Functional safety" as an international standard for road vehicles with electronic systems. Following ETSI TS 103 097 released in 2013 for intelligent transportation systems (ITS) security specifications, SAE J3061 is used as a cybersecurity guidebook for cyber-physical vehicle systems. It enables flexible, pragmatic, and adaptable applications to the vehicle industry and benefits other cyber-physical vehicle systems such as commercial and military vehicles, trucks, and busses. ISO/IEC 27000:2018 works for all organisations such as commercial enterprises and government agencies, which provides terms and definitions of information security management systems (ISMS). SOTIF (ISO/PAS 21448:2019) provides guidance on the practical design, verification and validation measures for intended functionality where situational awareness associated with complicated sensors and processing algorithms is deemed to be critical for the system safety. Then, other standards for the ITS in road transport are developed. For instance, Directive 2010/40/EU works for the ITS and the interfaces with other modes of transport. More recently, cybersecurity risks have attracted the interest of the industry. ISO/SAE 21,434 is a baseline to ensure that cybersecurity risks are managed efficiently and effectively. As a result, safety and security are well set based on the final impact on the driver.

As shown in the upper line, there were relatively fewer initiatives on SSCA in railway transport. Positive train control (PTC) is a train protection system to control the system in case of positive movement allowance, which generally improves railway traffic safety. EN 50,159 standard illustrates the basic requirements to enable safe communication between safety-related components connected to the transmission system, which is referred to when the system safety analysis needs to be integrated with security hazards (Bezzateev et al., 2013). In addition, NEN-EN 50129:2016 focuses on Reliability, Availability, Maintainability, and Safety (RAMS) of railway transportation (CENELEC). BS EN 50129:2018 works for railway signalling applications and applies to generic systems defining a class of applications. However, it does not include the aspects of the occupational health and safety of personnel. Hence, there are not many railway studies concentrating on investigating initiatives of safety and security. However, risk perceptions from the travellers and passengers were more focused on given security breaches (Nordfjaern et al., 2015; Coppola and Silvestri, 2021). In other words, the SSCA in railway transport relies more on the ultimate users than the transport process. Therefore, there is a tendency to integrate the passenger's perception of security and safety into the co-analysis in railway transport.

As shown in the lower line, the SSCA initiatives span a wide range of time periods as far as maritime transportation is concerned. Starting from 1974, the International Convention for the Safety of Life at Sea (SOLAS) works as an international maritime treaty that sets minimum safety standards in merchant ships' construction, equipment, and operation. Followed by the releases of the

International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) in 1978 and the Pilotage Act in 1987, the International Safety Management (ISM) Code came into force in 1993 to provide a standard for the safe management and operation of ships at sea. It benefits the ship safe management and pollution prevention. For the security issues, the International Ship and Port Facility Security Code (ISPS Code) came into force in 2004, which is an amendment to SOLAS Convention (1974/1988) on Maritime security, including minimum security arrangements for ships, ports and government agencies. It proposes that governments, shipping companies and personnel should "detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade." This initiative was also referred to as a method for quantifying port-security performance (Antão et al., 2016). In 2010, STCW Manila Amendments defined new training requirements for all seafarers, which was utilised to design and evaluate training scenarios for maritime safety and security (Baldauf et al., 2012). Moreover, Port Marine Safety Code (PMSC) sets out a national standard for port marine safety. It has been applied to all harbour authorities and other marine facilities, berths and terminals in the UK. The first time that safety-security indicators presented in maritime transport was during a meeting by the ESPO Marine Affairs and Security (MA&S) committee in Kolding (Denmark) on the 29th April 2014 (Antão et al., 2016). The representatives who attended the meeting were from various ports and organisations, including Transport Malta, Transport Gruppen, and the Finish Ports Association. It has raised the concerns about SSCA and on how to mitigate the barriers influencing the integration of safety and security. It was followed by the second MA&S committee workshop and then a meeting in 2015. It illustrates the need for integrating safety and security in the maritime sector. Furthermore, maritime transportation encounters a challenge of the transition from traditional shipping circumstances to an intelligent cyber-physical environment. Although some efforts have been made, such as introducing the ISPS code, there are many issues for cyber-physical systems development, referring to the evolution process of road transportation.

Regarding initiatives of multimodal transportation, it is evident that road transport is the most advanced field in terms of SSCA initiatives, while the maritime sector has the longest history of releasing relevant standards. Given the rising automation and cyber-security systems, it is evident that railway transport and maritime fields witness the fast development of new security-oriented initiatives. The railway transport could learn lessons from road transport which develops the cybersecurity guidebook for cyber-physical systems in terms of transport process. At the same time, the maritime sector needs to further develop security code and/or SSCA regulations aiming at autonomous ships, which can be learned from the road sector with the ITS rules. Also, it is evident that security standards follow the development of safety initiatives. It is inevitable to integrate security with safety to the robust development of multimodal transport from a systematic perspective.

The regulatory development integrated with literature review implies the trend of applying SSCA into autonomous technologies in terms of a single transportation system or multimodal transportation. Intelligent transportation systems and driverless vehicles are hot topics in road transportation and are highly relevant to public transport, including smart cities and intelligent infrastructures. Because transportation systems have been equipped with wireless connections and digital techniques, cyber-physical systems inherently require a high-security level as any malicious digital attack in communications and information transmissions could cause catastrophic accidents. In that way, the requirement of SSCA grows along with the development of autonomous transport systems in the near future.

The security initiatives will be emphasised to meet the demand of CPSs. The security onboard driverless buses revealed more concerns than their traffic safety (Salonen, 2018). It illustrates the importance of security enhancement in the process of the design and operations of autonomous vehicles. The cyber-enabled ship interconnected with CPSs, needs to take into account security issues and system safety at the design stage of the system (Kavallieratos et al., 2020). Therefore, the autonomous development of transportation systems will require discussions on the SSCA. The proposed framework in Fig. 7 sets a possible research agenda for the SSCA of autonomous transport systems at their design stages.

From an applied research perspective, SSCA provides insights into policy-making, operator training, and accident prevention. The risk perception study on SSCA explains the perceived safety and security under different circumstances with various criteria. It can stimulate comprehensive risk assessment in public transport. The SSCA can provide the beneficiaries (e.g. policymakers) with a guideline to further explore the complementation of various methods analysed in Section 4.2 and enrich the SSCA framework for its applications in practice. Effective education and training in SSCA will benefit operators and improve their safety performance. In such a way, they will enhance their working skills and deal with hazards at an early stage before they lead to systems failures or accidents/incidents. As far as the accident investigation is concerned, the conventional safety investigation into accidents is not practical for the complicated interactions in SoS in terms of emerging security threats (e.g. malicious attacks). New bottom-up approaches proposed in Fig. 7 should be further investigated to aid accident investigators to detect security failures and more importantly, present and compare such security failures with the safety ones to allow the development of the cost effective control measures that can reduce the risk levels of both failures simultaneously.

6. Conclusions and future directions

SSCA is beneficial in transportation in the fast growing digitalisation and automation era. To eliminate the barriers in SSCA development, this study reviews the literature on the SSCA and compares their applications across different transport modes regarding systematic models. Based on advantages of various analysis methods, a conceptual framework is proposed to imply insights for the SSCA through a combined top-down and bottom-up approach, followed by a case study. Then the initiative/regulatory analysis is conducted to reveal the current development of safety and security in practice from different transport modes and help consolidate the interrelations among them in regulatory standards. The novelty of this paper lies in a conceptual SSCA framework by integrating advantages of both security-driven and safety-driven methods, followed by a case study using FER to investigate the SSCA of seaports. In light of the case study, the ER's characteristic of synthesising risk results from different perspectives (e.g., safety and security)

ensures the possibility of combining the safety/security analysis results from different transport modes involved in a system. However, the limitation of this study is that some risk-related methods have not been included in this paper, as this work's focus is currently set on the ones that make the most contributions to both safety and security risk analysis. Some findings (e.g. Fig. 6) are strictly drawn based on the literature review; they could be further extended when new data/evidence becomes available.

In addition, the proposed SSCA framework highlights its potential in facilitating safety and security co-analysis and illustrates that safety and security risk analysis and management practices across different transport modes can be cross-fertilised. The SSCA framework will introduce substantial benefits, including a regime that addresses both safety and security in an integrated and quantitative manner; guidance on regulatory requirements for policy makers; and a proactive approach, properly considering the hazards and threats of transport systems. It integrates hazards of the system and failure mode of components to analyse how things go wrong and illustrate vulnerability in the system, which implies the process of factors interacting with each other to lead to the accident/incident. Next, the proposed control measures and safety/security requirements provide clues on how resources and strategies intervene in the system to ensure as many things as possible go right. That is to say, the findings and results can aid in generating reliable and rational recommendations to make things go right within the context of Safety II. Along with the new findings and implications, this paper identifies the following research directions that can further improve SSCA in transportation, requiring more research outlooks in the future.

1) Autonomous industrial development in transportation systems.

There is a novel trend for the transport system to be studied with interconnected intelligent techniques and infrastructures. Since 2007, ITS for the vehicle and automated control systems for the railway has shown the increasing demands for complex systems to consider the security breaches into conventional safety assessment. Although the autonomous development of the maritime sector is relatively later than other sectors, autonomous ships and cyber-physical systems attract significant interest in SSCA. It includes designing the system, identifying hazards hidden behind the application of new techniques, and training the crews given new challenges in the autonomous industry (Fagnant and Kockelman, 2015). In addition, autonomous or smart ports that implementing smart technologies to maintain safe, secure, and energy efficient facilities are developing fast, such as utilising information and communications technology to improve vessels and container management (Yau et al., 2020), and employing an autonomous underwater vehicle (AUV) as a towed vehicle for the port area inspection (Choi et al., 2007). The high-perfromance port supply chain, such as Xiamen port and Shanghai Yangshan port, reveals the trend of utilising autonomous technology and sustainable strategies to realise the digital revolution (Wu et al., 2019; Liu et al., 2022). Maritime transport can borrow lessons from autonomous ports to obtain better performance. Both bottom-up and top-down approaches will need to be further investigated for autonomous vehicles and intelligent technology in complex systems (Li et al., 2019).

2) Interconnectivity of transport systems.

Through the analysis on concepts of SSCA, both safety-oriented and security-oriented co-analysis show the interconnectivity between various parameters and indicators among system components (Hernandez et al., 2016). Some safety issues and security breaches can be identified separately, followed by integrating analysis of the performance of target systems. However, more work should be conducted to explore the system safety and security KPIs simultaneously using a systematic model. The combined list of the KPIs can capture the system risk's dynamic characteristics and solves potential conflicts of both aspects for better risk control of transport systems. In this way, more systematic models need to be developed to deal with the conflicts between this safety and security analysis methods. In addition, SSCA and risk control measures should be developed within the context of multimodal transport systems. It will allow for the analysis and management of the safety and security risks at different transport modes, but within the same supply chain systematically.

3) Cyber-security/intelligent cyber-physical systems.

Aiming at realising the rational decision making at the high-level hierarchy of a system, previous SSCA research presents frameworks and conceptual works by reviewing regulations and rules. However, the increasing application of information technology and the accordant proliferation of interacted CPSs has given rise to security and safety issues and challenges (Kavallieratos et al., 2020; Cheung et al., 2021). More research will propose integrated methods for safety and security engineering for CPSs at the system design stage. The autonomous design and lifecycle assessment requires the clear identification of coherent, consistent, and non-conflicting security and safety requirements. To tackle the rising profile of intelligent cyber-physical systems in autonomous transport systems in future, the SSCA framework will help define their safety and security objectives and identify the relevant requirements.

4) Fault tolerance systems.

A complex transport system consists of various sub-systems, and the complexity could grow with the use of more autonomous techniques. The traditional way of investigating risks and hazards can only help tackle the classical mistakes and failures known in full or in part and will be incompetent to non-classical risks such as cyber-attacks. However, the resilience of a transport system can only be obtained by capturing the dynamic system characteristics when facing both classical and non-classical risks. Such system characteristics often reveal the fault tolerance demands for transportation. As a cyber-physical system, the SSCA in transportation needs to carefully measure the fault tolerance of systems so as to accommodate the conflicts among components, respond to disturbances of attributes (Parajuli et al., 2021), and recover from unstable situations caused by attacks and risks. In addition, new initiatives have to be developed to address the safety and security requirements of multimodal transport chains holistically.

CRediT authorship contribution statement

Shiqi Fan: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Project administration. **Zaili Yang:** Conceptualization, Methodology, Validation, Investigation, Resources, Writing – original draft, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the European Research Council under Grant [Number TRUST CoG 2019 864724].

References

Abeyratne, R., 2012. Acceptance of human remains for carriage by air- some concerns in security and safety. Journal of Transportation Security 5, 305–317.
Abeyratne, R., 2014. Flight MH 17 and state responsibility for ensuring safety and security of air transport. Journal of Transportation Security 7, 347–357.
Acheampong, R.A., 2021. Societal impacts of smart, digital platform mobility services-an empirical study and policy implications of passenger safety and security in ride-hailing. Case Studies on Transport Policy 9, 302–314.
Alam, M.W., Xu, X.M., Ahamed, R., Mozumder, M.M.H., Schneider, P., 2021. Ocean governance in Bangladesh: Necessities to implement structure, policy guidelines, and actions for ocean and coastal management. Regional Studies in Marine Science 45, 101822.
ALYAMI, H., YANG, Z., RAMIN, R., BONSALL, S., WANG, J., WAN, C. & QU, Z. 2022. Selection of safety measures in container ports. *International Journal of Shipping and Transport Logistics,* Accepted for press.
Alyami, H., Lee, P.-T.-W., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2014. An advanced risk analysis approach for container port safety evaluation. Maritime Policy & Management 41, 634–650.
Alyami, H., Yang, Z., Riahi, R., Bonsall, S., Wang, J., 2019. Advanced uncertainty modelling for container port risk analysis. Accident Analysis & Prevention 123, 411–421.
Antão, P., Calderón, M., Puig, M., Michail, A., Wooldridge, C., Darbra, R.M., 2016. Identification of Occupational Health, Safety, Security (OHSS) and Environmental Performance Indicators in port areas. Safety Science 85, 266–275.
Baldauf, M., Schröder-Hinrichs, J.U., Benedict, K., Tuschling, G., 2012. Simulation-based team training for maritime safety and security. Journal of Maritime Research 9, 3–9.
BEN HAMIDA, E., JAVED, M. A. & ZNAIDI, W. 2017. Adaptive security provisioning for vehicular safety applications. *International Journal of Space-Based and Situated Computing,* **7,** 16-31.
BEZZATEEV, S., VOLOSHINA, N., SANKIN, P. & IEEE 2013. Joint Safety and Security Analysis for Complex Systems. *Proceedings of the 2013 13th Conference of Open Innovations Association.*
BOLBOT, V., THEOTOKATOS, G., WENNERSBERG, L. A., FAIVRE, J., VASSALOS, D., BOULOUGOURIS, E., RODSETH, O. J., ANDERSEN, P., PAUWELYN, A. S. & VAN COILLIE, A. 2021. A novel risk assessment process: Application to an autonomous inland waterways ship. *Proceedings of the Institution of Mechanical Engineers Part O-Journal of Risk and Reliability***,** 1748006X211051829.
Branscomb, L.M., Ellis, R.N., Fagan, M., 2012. Between Safety and Security: The Policy Challenges of Transporting Toxic Inhalation Hazards. Journal of Homeland Security and Emergency Management 9.
CHEN, D., MEINKE, K., OSTBERG, K., ASPLUND, F. & BAUMANN, C. A knowledge-in-the-loop approach to integrated safety & security for cooperative system-of-systems. 7th IEEE International Conference on Intelligent Computing and Information Systems, ICICIS 2015, 2016. 13-20.
Cheung, K.-F., Bell, M.G., Bhattacharjya, J., 2021. Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review 146, 102217.
Choi, J.K., Shiraishi, T., Tanaka, T., Sakai, H., 2007. A practical and useful autonomous towed vehicle for port area inspection. Advanced Robotics 21, 351–370.
Coppola, P., Silvestri, F., 2020. Assessing travelers' safety and security perception in railway stations. Case Studies on Transport Policy 8, 1127–1136.
Coppola, P., Silvestri, F., 2021. Gender Inequality in Safety and Security Perceptions in Railway Stations. Sustainability 13, 4007.
Daziano, R.A., Rizzi, L.I., 2015. Analyzing the impact of a fatality index on a discrete, interurban mode choice model with latent safety, security, and comfort. Safety Science 78, 11–19.
Dghaym, D., Hoang, T.S., Turnock, S.R., Butler, M., Downes, J., Pritchard, B., 2021. An STPA-based formal composition framework for trustworthy autonomous maritime systems. Safety Science 136, 105139.
Dong, H.R., Ning, B., Chen, Y., Sun, X.B., Wen, D., Hu, Y.L., Ouyang, R.H., 2013. Emergency Management of Urban Rail Transportation Based on Parallel Systems. Ieee Transactions on Intelligent Transportation Systems 14, 627–636.
Enoma, A., Allen, S., 2007. Developing key performance indicators for airport safety and security. Facilities 25, 296–315.
Ericson, C.A., 2015. Hazard analysis techniques for system safety. John Wiley & Sons.
ERIK NILSEN, T., LI, J., JOHNSEN, S. O. & GLOMSRUD, J. A. 2018. Empirical studies of methods for safety and security co-analysis of autonomous boat. *Safety and Reliability-Safe Societies in a Changing World,* 2949-2957.
Fagnant, D.J., Kockelman, K., 2015. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transportation Research Part a-Policy and Practice 77, 167–181.
Fox, S., 2014. Safety and security: The influence of 9/11 to the EU framework for air carriers and aircraft operators. Research in Transportation Economics 45, 24–33.
Gromule, V., Yatskiv, I., Pēpulis, J., 2017. Safety and security of passenger terminal: the case study of Riga International Coach Terminal. Procedia Engineering 178, 147–154.
Guthrie, K., 2011. The role of civil aviation safety and security in the economic development of Pacific Island countries. Journal of Social, Political, and Economic Studies 36, 218–248.
Guzman, N.C.H., Wied, M., Kozine, I., Lundteigen, M.A., 2020. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Systems Engineering 23, 189–210.
Hawila, M.A., Chirayath, S.S., 2018. Combined nuclear safety-security risk analysis methodology development and demonstration through a case study. Progress in Nuclear Energy 105, 153–159.
HERING, H., HAGMÜLLER, M. & KUBIN, G. Safety and security increase for air traffic management through unnoticeable watermark aircraft identification tag transmitted with the VHF voice communication. The 22nd Digital Avionics Systems Conference - Proceedings, 2003 Indianapolis, IN. 4.E.2/1-4.E.2/10.
Hernandez, S., Monzon, A., de Ona, R., 2016. Urban transport interchanges: A methodology for evaluating perceived quality. Transportation Research Part a-Policy and Practice 84, 31–43.

Ipingbemi, O., Aiworo, A.B., 2013. Journey to school, safety and security of school children in Benin City, Nigeria. Transportation Research Part F-Traffic Psychology and Behaviour 19, 77–84.
Javed, M.A., Hamida, E.B., 2017. On the Interrelation of Security, QoS, and Safety in Cooperative ITS. IEEE Transactions on Intelligent Transportation Systems 18, 1943–1957.
Jiang, M.Z., Lu, J., 2020. The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. Transportation Research Part E-Logistics and Transportation Review 139, 101965.
John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R., Wang, J., 2014. An integrated fuzzy risk assessment for seaport operations. Safety science 68, 180–194.
Johnston, R.G., 2004. Adversarial safety analysis: Borrowing the methods of security vulnerability assessments. Journal of Safety Research 35, 245–248.
Kavallieratos, G., Katsikas, S., Gkioulos, V., 2020. SafeSec Tropos: Joint security and safety requirements elicitation. Computer Standards & Interfaces 70, 103429.
Kesseler, E., 2004. Integrating air transport elicits the need to harmonise software certification while maintaining safety and achieving security. Aerospace Science and Technology 8, 347–358.
KORNECKI, A. J., SUBRAMANIAN, N. & ZALEWSKI, J. Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks. 2013 Federated Conference on Computer Science and Information Systems, 2013. IEEE, 1393-1399.
Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety 139, 156–178.
KUBOTA, S., OKAMOTO, Y. & ODA, H. Study of security of driving safety support system using RFID. 7th International Conference on Intelligent Transport Systems Telecommunications, ITST 2007, 2007 Sophia Antipolis. 236-239.
LAUTIERI, S., COOPER, D. & JACKSON, D. 2005. *SafSec: Commonalities between safety and security assurance*.
Leveson, N.G., Thomas, J.P., 2018. STPA handbook. Massachusetts Institute of Technology, Cambridge.
Li, S.X., Sui, P.C., Xiao, J.S., Chahine, R., 2019. Policy formulation for highly automated vehicles: Emerging importance, research frontiers and insights. Transportation Research Part a-Policy and Practice 124, 573–586.
Lisova, E., Sljivo, I., Causevic, A., 2019. Safety and Security Co-Analyses: A Systematic Literature Review. Ieee Systems Journal 13, 2189–2200.
Liu, Y., Zhou, Z.Y., Yang, Y.S., Ma, Y., 2022. Verifying the Smart Contracts of the Port Supply Chain System Based on Probabilistic Model Checking. Systems 10, 19.
Mansor, H., Fadzir, T.M.A.M., Gunawan, T.S., Janin, Z., 2019. Safety and security solution for school bus through RFID and GSM technologies. Indonesian Journal of Electrical Engineering and Computer Science 17, 804–814.
Marquez, L., Soto, J.J., 2021. Integrating perceptions of safety and bicycle theft risk in the analysis of cycling infrastructure preferences. Transportation Research Part a-Policy and Practice 150, 285–301.
Muller, P.J., Young, S.E., Vogt, M.N., 2007. Personal rapid transit safety and security on university campus. Transportation Research Record 95–103.
Nordfjaern, T., Lind, H.B., Simsekoglu, O., Jorgensen, S.H., Lund, I.O., Rundmo, T., 2015. Habitual, safety and security factors related to mode use on two types of travels among urban Norwegians. Safety Science 76, 151–159.
NOVAK, T., TREYTL, A. & PALENSKY, P. Common approach to functional safety and system security in building automation and control systems. 2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007), 2007. IEEE, 1141-1148.
Olfindo, R., 2021. Transport accessibility, residential satisfaction, and moving intention in a context of limited travel mode choice. Transportation Research Part a-Policy and Practice 145, 153–166.
Olojede, O., Daramola, O., Olufemi, B., 2017. Metropolitan transport safety and security: An African experience. Journal of Transportation Safety and Security 9, 383–402.
Ou, Z.Q., Zhu, J.J., 2008. AIS Database Powered by GIS Technology for Maritime Safety and Security. Journal of Navigation 61, 655–665.
Parajuli, A., Kuzgunkaya, O., Vidyarthi, N., 2021. The impact of congestion on protection decisions in supply networks under disruptions. Transportation Research Part E: Logistics and Transportation Review 145, 102166.
Patriarca, R., di Gravio, G., Woltjer, R., Costantino, F., Praetorius, G., Ferreira, P., Hollnagel, E., 2020. Framing the FRAM: A literature review on the functional resonance analysis method. Safety Science 129, 104827.
PAWLIK, M. 2016. Communication Based Train Control and Management Systems Safety and Security Impact Reference Model. *In:* MIKULSKI, J. (ed.) *Challenge of Transport Telematics, Tst 2016*.
PAWLIK, M. 2018. Application of the Safety and Security Impact Reference Model for Communication Based Train Control and Management Systems. *In:* MIKULSKI, J. (ed.) *Management Perspective for Transport Telematics*.
Potoglou, D., Robinson, N., Kim, C.W., Burge, P., Warnes, R., 2010. Quantifying individuals' trade-offs between privacy, liberty and security: The case of rail travel in UK. Transportation Research Part a-Policy and Practice 44, 169–181.
Raspotnig, C., Karpati, P., Katta, V., 2012. A combined process for elicitation and analysis of safety and security requirements. *Enterprise, business-process and information systems modeling*. Springer.
Salonen, A.O., 2018. Passenger's subjective traffic safety, in-vehicle security and emergency management in the driverless shuttle bus in Finland. Transport Policy 61, 106–110.
SCHMITTNER, C., GRUBER, T., PUSCHNER, P. & SCHOITSCH, E. Security application of failure mode and effect analysis (FMEA). International Conference on Computer Safety, Reliability, and Security, 2014a. Springer, 310-325.
SCHMITTNER, C., MA, Z. & SMITH, P. FMVEA for safety and security analysis of intelligent and cooperative vehicles. International Conference on Computer Safety, Reliability, and Security, 2014b. Springer, 282-288.
Schmittner, C., Ma, Z., Puschner, P., 2016. Limitation and improvement of STPA-Sec for safety and security co-analysis. In: International Conference on Computer Safety, Reliability, and Security. Springer, pp. 195–209.
SHARMA, S., FLORES, A., HOBBS, C., STAFFORD, J. & FISCHMEISTER, S. Safety and Security Analysis of AEB for L4 Autonomous Vehicle Using STPA. Workshop on Autonomous Systems Design (ASD 2019), 2019. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.
Steenbruggen, J., Borzacchiello, M.T., Nijkamp, P., Scholten, H., 2013. Data from telecommunication networks for incident management: An exploratory review on transport safety and security. Transport Policy 28, 86–102.
TBATOU, S., RAMRAMI, A. & TABII, Y. Security of communications in connected cars modeling and safety assessment. 2nd International Conference on Big Data Cloud and Applications, BDCA 2017, 2017.
Tokody, D., Albini, A., Ady, L., Rajnai, Z., Pongracz, F., 2018. SAFETY AND SECURITY THROUGH THE DESIGN OF AUTONOMOUS INTELLIGENT VEHICLE SYSTEMS AND INTELLIGENT INFRASTRUCTURE IN THE SMART CITY. Interdisciplinary Description of Complex Systems 16, 384–396.
TORKILDSON, E. N., LI, J., JOHNSEN, S. O. & GLOMSRUD, J. A. 2018. Empirical studies of methods for safety and security co-analysis of autonomous boat. *Safety and Reliability-Safe Societies in a Changing World*.
Török, Á., Pethő, Z., 2020. Introducing safety and security co-engineering related research orientations in the field of automotive security. Periodica Polytechnica Transportation Engineering 48, 349–356.
Urbanski, J., Morgas, W., Kopacz, Z., 2008. The safety and security systems of maritime navigation. Journal of Navigation 61, 529–535.
Van Asselt, M.B.A., 2018. Safety in international security: a view point from the practice of accident investigation. Contemporary Security Policy 39, 590–600.
Vlissidis, N., Leonidas, F., Giovanis, C., Marinos, D., Aidinis, K., Vassilopoulos, C., Pagiatakis, G., Schmitt, N., Pistner, T., Klaue, J., 2017. A sensor monitoring system for telemedicine, safety and security applications. International Journal of Electronics 104, 297–311.
Wu, X.F., Zhang, L.P., Dong, Y.W., 2019. Towards sustainability in Xiamen Harbor, China. Regional Studies in Marine Science 27, 100552.
Yang, Z., Bonsall, S., Wang, J., Fang, Q., Yang, J., 2005. Subjective risk assessment of container supply chains. International Journal of Automation and Computing 2, 20–28.
Yang, Z., Ng, A.K., Wang, J., 2013. Prioritising security vulnerabilities in ports. International Journal of Shipping and Transport Logistics 5, 622–636.
Yang, Z., Ng, A.K., Wang, J., 2014. A new risk quantification approach in port facility security assessment. Transportation research part A: policy and practice 59, 72–90.

Yang, Z., Qu, Z., 2016. Quantitative maritime security assessment: a 2020 vision. IMA Journal of Management Mathematics 27, 453–470.
Yang, Z.L., Wang, J., Bonsall, S., Fang, Q.G., 2009. Use of fuzzy Evidential Reasoning in maritime security assessment. Risk Analysis 29, 95–120.
Yau, K.L.A., Peng, S.H., Qadir, J., Low, Y.C., Ling, M.H., 2020. Towards Smart Port Infrastructures: Enhancing Port Activities Using Information and Communications Technology. Ieee Access 8, 83387–83404.
YOUNG, W. & LEVESON, N. Systems thinking for safety and security. Proceedings of the 29th Annual Computer Security Applications Conference, 2013. 1-8.
Zhou, X.Y., Liu, Z.J., Wang, F.W., Wu, Z.L., 2021. A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Engineering 222, 108569.