2022-11

Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime

Kayisoglu, G

10.1017/s0373463322000534
Journal of Navigation
Cambridge University Press (CUP)

The Journal of Navigation (2022), **75**:6 1364–1388
doi:10.1017/S0373463322000534

RESEARCH ARTICLE

Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime

Gizem Kayisoglu,[1]* Pelin Bolat,[2] and Kimberly Tam[3]

[1] Department of Maritime Transportation Management Engineering, Istanbul Technical University Maritime Faculty, Istanbul, Turkey
[2] Department of Basic Sciences, Istanbul Technical University Maritime Faculty, Istanbul, Turkey
[3] School of Engineering, Computing, and Mathematics, University of Plymouth, Plymouth, UK.
*Corresponding author. E-mail: yukselg@itu.edu.tr

Received: 21 June 2022; **Accepted:** 12 September 2022; **First published online:** 5 October 2022

Keywords: ECDIS cybersecurity; human error probability; SLIM; maritime cybersecurity

Abstract

There is an undeniable recognition that maritime cybersecurity risk management should involve process, technology, and people. However, thus far, most studies have focused on the technical and process aspects of maritime cybersecurity, more than on the human element. On a vessel, the Electronic Chart Display and Information System (ECDIS) is, amongst all the electronic devices on the bridge, a complex and indispensable maritime sociotechnical system that must consider both technical and human aspects. In the context of maritime cyber resilience, it is important to note that when developing strategies for maritime cybersecurity, one cannot only consider technical security measures and ignore human error, as this does not adhere to good cybersecurity practice. To address this, this study aims to identify the navigating officers' responsibilities for ECDIS cybersecurity and find the human error probabilities during these tasks via the SLIM-based human reliability analysis method. The outputs of this study provide an insight for industrial policies and best practices, in ECDIS cybersecurity risk management in terms of the behavioural and cultural aspects of shipping.

1. Introduction

The high level of digitalisation and connectivity in the maritime sector makes the cybersecurity issue a significant one. Specifically, the cyber environment of ships contain interconnected networks of both Information Technologies (IT) and Operational Technologies (OT) (Gunes et al., 2021). This cyber space onboard provide services, information, business and social functions. To ensure the continued security and safety of these functions, there is an agreement that human capabilities and human strengths, when working together, are key for the management of cyber vulnerabilities. Therefore, the human element is key in establishing and maintaining robust cybersecurity and in preventing cyber-attacks (White Paper, 2022).

Electronic Chart Display and Information System (ECDIS) is one critical asset, which integrates IT and OT, in the navigational bridge onboard ships (Kristic et al., 2021). It is an electronic device including software, hardware, data, and a human–machine interface (Weintrit, 2009). One requirement for ECDIS to be used onboard comes from the International Convention for the Safety of Life at Sea (SOLAS). This requirement states that all ships include the same or more functionality compared to paper navigational charts and main navigation specifications, published by International Maritime Organization (IMO) (IMO, 2006). According to on-board fulfilment requirements, ECDISs must be type approved; this requires that software must be maintained, including up-to-date Electronic Navigational

Charts (ENCs), and it must be installed with adequate backup arrangements for navigation safety (IHO, 2017, 2018; IMO, 2009, 2017a). ECDIS is integrated with a ship's sensors, satellite position fixing and other advanced electronic databases, including chart information. According to the IMO performance standards involving the configuration of ECDIS, the information of position, heading and speed are received from a global positioning system (GPS), which is the one of the global navigation satellite systems (GNSS), gyrocompass, and speed log, respectively, which are the mandatory systems integrated with ECDIS. In addition, ECDIS merges and synthesises the information received from other systems, such as radio detection and ranging (RADAR), automatic identification system (AIS), autopilot, and voyage data recorder (VDR) for safety of ship and environment. This communication uses a NMEA (National Marine Electronics Association; NMEA0183 Standard for Interfacing Marine Electronic Devices) interface (Weintrit, 2009; Svilicic et al., 2019b). ECDIS systems must also be kept updated according to the product specifications and presentation library of the International Hydrographic Organization (IHO) ENC by considering the latest version of them (OCIMF, 2020). Updating the ENC in time also procures creditable performance for ECDIS and carries a main precondition for safe of navigation (Weintrit, 2009).

Although there are apparent benefits, as mentioned, with the integration of several operational navigation equipment with ECDIS, the risk of cyber-attacks on the ECDIS system or its integrated items emerges. Because ECDIS and its typical back arrangement have high-level connectivity and digitalisation, they are an excellent environment for cyber-security threats associated with the distribution of malicious code (Svilicic et al., 2020). For this reason, cyber-attacks aimed directly at ECDIS or its integrated items should be considered as a critical issue to ensure safety of life, property and environment (Kristic et al., 2021). Moreover, OCIMF (2020) stated that ECDIS involves three category of vulnerabilities: (i) human factors and machine interface, (ii) ECDIS navigation procedures and practices, (iii) ECDIS hardware, software and ENC data. In this context, the issue of cybersecurity of ECDIS must consider the perspective of human factors, as well. Since ECDIS-related cyber incidents or any digital errors can occur due to people's over-reliance on technology, along with disrupted main navigational skills and weak situational awareness (Nielsen, 2016; BrčićSrđan et al., 2018; Tsimplis and Papadas, 2019), the human factor is important to consider.

Navigating officers and masters onboard a ships have various responsibilities over ECDIS operations. A list of key operations include, but are not limited to: setting up and maintaining display, operational use of electronic charts, route planning, route monitoring, alarm handling, manual correction of a ship's position and motion parameters, records in the ship's log, chart updating, operational use of ECDIS with radar/ARPA connected, operational use of ECDIS where AIS connected, operational warnings, their benefits and limitations, and system operational tests (Weintrit, 2009). These tasks are not performed by the navigating officers or masters according to a hierarchical order. The performance of these tasks depends on the necessities of navigation, international maintenance requirements, intervals of charts updating, manufacturers' technical bulletins, and similar issues.

As these tasks are carried out by navigating officers and masters, cyber-attacks or incidents derived from human error commission/omission can occur. For instance, a malicious software can infiltrate all onboard navigation systems via USB drive plugged into the ECDIS by a navigating officer, if the navigating officer does not use specially designated and pre-scanned USBs. As a result of this, ECDIS sensor data can be manipulated with unreliable information displayed to the officer of the watch, some false alerts can appear, and the system can be critically slowed down (PaSea, 2018). Similarly, during ENC updating on the internet without any checking security of system, unauthorised logical access can be used to attack ECDIS and all navigation systems (Svilicic et al., 2019d). Additionally, if navigating officers do not take any precautions against physical access to ECDIS, unauthorised physical access could be possible. Therefore, files, routes or other significant information can be changed, deleted or send to the unwanted third parties.

Based on these facts, it can be said that ECDIS consists of two strengths, the first of which is the design leading to vulnerabilities to possible malicious attacks and human error. These strengths of ECDIS provides several opportunities, such as safety of navigation and maritime situational awareness.

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

The weaknesses of ECDIS can result in various threats, which can create dangers for the safety of navigation, maritime surveillance and responsibilities of navigating officers for decision-making situations.

To prevent these threats, ensuring and improving cyber resilience onboard, IMO adopted MSC.428 resolution, which is *Marine Cyber Risk Management in Security Management System* (SMS) (IMO, 2017b) and *Guidelines on Cyber Risk Management* (MSC-FAL 1/Circ.3) (IMO, 2017c). These documents required that all ship's safety management system should include cyber risks and ways to protect ships and ship systems from cyber-attacks in the context of International Safety Management Code (ISM) until 1 January 2021. In accordance with these requirements, although cyber-security clauses including ECDIS already exist in the Safety Management Manuals (SMM) onboard ships, it is seen that detailed cyber responsibilities and procedures as systematically for general cyber spaces onboard ships including ECDIS have not been encountered. On the other hand, in maritime cybersecurity, several available standards, policies and guidelines, such as International Electrotechnical Commission (IEC) 61162-1, IEC 61162-2, IEC 27005, IEC 61162-450, NIST framework, the guidelines on cyber-security onboard ships, and code of practice cybersecurity for ships, only present the recommendations from the technical aspects, such as from the perspective of physical, application, network, data security and requirements of usage of security (BS EN IEC 61162-1, 1996; BS EN IEC 61162-2, 1999; BS ISO-IEC 27005, 2011; ICS and other organizations, 2016; BS EN IEC 61162-450, 2018; NIST, 2020). However, not all these resources focus on cyber responsibilities in maritime in an effective way. By considering these aspects, the tasks of navigating officers related to bridge navigation and communication assets, specifically ECDIS operations, have must be reshaped according to cyber-security requirements for IT and OT cyber onboard, since cybersecurity in maritime is a comparatively new touchstone for safe navigation at sea. In other words, the tasks of navigating officers have evolved to not only consider to requirements of operations, but to also consider cyber-security measurements regarding related operations. However, these duties, which are blended with the requirements of cybersecurity on ships, cannot be implemented effectively and in a standard way by all officers on board because of customary navigation culture, with overreliance on technology and the problem of adaptation to the fulfilment of technological measures with tasks, the lack of training (standard or tailored), awareness, experience.

Most cybersecurity incidents or attacks against ships are the result of human error. As a result of cyber-attacks, collisions, grounding or sinking can cause serious harm to life, property and the environment. This harm can be caused due to access hackers obtain to monitoring and control systems onboard and manipulation of navigation system. Other outcomes include financial loss, extortion and damage to a company's reputation, for example if sensitive information onboard is stolen. To prevent such calamities, it is critical for navigating officers to have the ability and performance skills to complete at a reasonable speed an efficient ECDIS operation while considering cyber-security measurements. At this point, the expectation from navigating officers is to perform their tasks without any navigational, operational or technical malfunctions. Hence, determining the probability of human error for each ECDIS-related task during navigational and communication operations on a vessel while considering cybersecurity is critical to preventing these losses.

This study aims to identify the responsibilities of navigating officers and other related human factors relating to ECDIS cybersecurity and to determine the human error probabilities during these tasks via the success likelihood index method (SLIM)-based human reliability analysis (HRA) method. SLIM is a one of the expert-based HRA methods that is used to overcome existing lack of statistical, historical or recorded data related to a particular task. Due to the lack of historical data to understand human errors for ECDIS cyber-security tasks onboard ships, the SLIM method is considered in this study.

To the authors' best knowledge, a study that focuses on human error probabilities for ECDIS cybersecurity does not exist within existing literature. There are some academic studies that only include ECDIS cyber vulnerabilities and mitigation options from a technical perspective (Tam and Jones, 2018, 2019; Mraković and Vojinović, 2019; Svilicic et al., 2019b, 2019c) or involve suggestions on the importance of human factor and behaviour for maritime cybersecurity (DNV-GL, 2016; Hareide et al., 2018;

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 1. *Related studies in the literature.*

References	Focusing points of the studies
Human reliability analysis seems to be a common method in the literature to find human error probabilities for information security in general, although not in the maritime field.	
Evans et al. (2019)	Conducted an empirical study using the Information Security Core Human Error Causes (IS-CHEC) technique, which is an information security adaptation of Human Error Assessment and Reduction Technique (HEART) to perform human reliability analysis for recorded information security incidents within the participating public sector organization.
Pollock (2017)	Intended to develop a tool to gather data and apply the Human Factors Analysis and Classification System (HFACS) to create a methodology for human errors for information security.
Conversely, in the maritime sector, there are some studies involving maritime cyber risk perception (Larsen and Lund, 2021; Pseftelis et al., 2021), importance of human factor for maritime cybersecurity (Vistiaho, 2017; Version et al., 2020), and maritime cyber policy for mitigation considering of human factor (Tam and Jones, 2018).	
DNV (2016)	Recommended process, technology and people for ensuring cybersecurity in maritime. For the people item, they suggest different levels of training for onboard and onshore personnel, such as ship cybersecurity officers, company cybersecurity officers, or internal auditors, general awareness for all crew and personnel, defining roles and responsibilities of related personnel, and designing and performing emergency cyber drills.
DNV (2022)	Asked participants in a survey what were the difficulties associated with managing cybersecurity within the OT environment. According to the results, there is lack of understanding of the risk and lack of skilled personnel in terms of people aspect.
Larsen and Lund (2021)	Developed a model that focus on dimensions of cyber risk perception within the psychometric paradigm and cognitive biases in general, and in the maritime domain via systematic literature review. Presented a psychological model in order to investigate the humans' cyber risk perception in maritime.
Pseftelis et al. (2021)	Presented a survey for the Greek maritime community with the aim to investigate the human factors and the awareness stakeholders have about maritime cybersecurity. According to results of their study, there is no adequate perception about the main items of cybersecurity (availability, integrity, confidentiality) and the related information and communication technologies (ICT) for protecting from cyber-attacks, and it is confirmed that the human factor can contribute to maritime cybersecurity in a positive or negative way.
Hanzu-Pazara et al. (2019)	Performed a study aiming of understanding how the individual behaviour and beliefs can affect the safety and security of the ship cyber systems by using simulation techniques combined with role-playing and interviews. According to their results, they have suggested that the operators on bridge onboard should realise the difference between the private data and information used by the ship's vital systems by the support of the administrative system, the shipping companies and adequate warnings.

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 2. *Nomenclature.*

AIS	Automatic Identification System
ANOVA	Analysis of Variance
ECDIS	Electronic Chart Display and Information System
ENCs	Electronic Navigational Charts
GNSS	Global Navigation Satellite System
GPS	Global Positioning System (GPS)
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HRA	Human Reliability Assessment
IEC	International Electrotechnical Commission
IHO	International Hydrographic Organisation
IMO	International Maritime Organisation
ISO	International Organisation for Standardisation
IT	Information Technology
MSC	Maritime Safety Committee
NMEA	National Marine Electronics Association
NtMs	Notices to Mariners
OT	Operational Technology
PSF	Performance Shaping Factors
RADAR	Radio Detection and Ranging
SLI	Success Likelihood Index
SLIM	Success Likelihood Index Method
SMS	Safety Management System
SOLAS	International Convention for the Safety of Life at Sea
STCW	International Convention on Standards of Training, Certification and Watch Keeping for Seafarers
THERP	Technique of Human Error Rate Prediction
VDR	Voyage Data Recorder

Lagouvardou, 2018; Tam and Jones, 2018; Hanzu-Pazara et al., 2019; Larsen and Lund, 2021; Pseftelis et al., 2021). The current state-of-the-art studies in the literature and their key points are listed in Table 1.

Contrary to the state-of-the-art literature, this paper focused on finding human error probabilities for ECDIS cybersecurity and, accordingly, developing strategies for related parts in maritime activities different from other studies.

All in all, the output of this study provides insights for the navigating officers, shipping companies managers or owners, ECDIS manufacturers, marine insurers and other related stakeholders in terms of improving cybersecurity within safety management manuals by considering bridge officers' cyber responsibilities, especially for ECDIS. This may include ECDIS cyber management plans under the ISM system of ships, designing information sharing policies and process between ECDIS manufacturers, shipping company, and ship, considering cyber responsibilities for ECDIS by marine insurers, and placing them in newly developed maritime cyber insurance policies. In this context, it is important to develop a comprehensive formed task list in order to ensure cyber resilience of all cyber spaces onboard a ship in the context of SMS.

The paper's design is as follows. Section 1 discusses the motivation and brief literature reviewing human reliability analysis and ECDIS cybersecurity in the maritime. The method process of this study is explained in Section 2. Section 3 shows the model application applied to ECDIS cybersecurity. The conclusions and contributions are given in Section 4. Finally, the acronyms and nomenclature within this paper is presented in Table 2 for easy reading.

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

2. Methodology

2.1. Success likelihood index method (SLIM)

Embrey et al. (1984a, 1984b) developed SLIM for measuring the probability of human error that emerges during the practice of a particular task. SLIM is an expert-based HRA method. Expert-based HRA methodologies are used when there is a lack of statistical, historical or recorded data related to a particular task. This is the case for many cyber-related tasks, as cybersecurity is a very recent issue with a small set of historical data.

The most commonly used expert-based HRA methodologies are SLIM, the technique of human error rate prediction (THERP), and the human error assessment and reduction technique (HEART) (Kayisoglu et al., 2022). These are all the first-generation methods developed for HRA. Therefore, they only consider the skill-based and rule-based activities, and their disadvantage is not to consider other factors, such as organisational factors, the impact of context and errors of commission (Norazahar, 2020). However, their critical advantages shine when applied to operational, maintenance and incident analysis for specific tasks or scenarios. In this case, human behaviour is based on skills, procedures and knowledge. In particular, SLIM depends on knowledge of experts that is a group for arguing specific tasks, and performance-shaping factors (PSFs) affect the success of tasks. The framework of the PSF is created on human factors performance based on expert opinion. The algorithm of SLIM is easy to apply and allows fast human error probability (HEP) for any specific task or scenario (Calixto, 2016). In this context, the most useful method can be considered as SLIM for understanding overall HEP of any particular task sequence, which have not been tacked before and lack data, and their PSF effects. Moreover, at the end of SLIM method, the possibility of errors which can happen in a specific operation can be decreased by developing and arranging PSFs within the system that procured an improvement in all safety levels. Contrary to this, the THERP method is more useful for understanding an event tree model and complex graphic representation for complex tasks. However, it omits the human PSFs, which impacts human error positively or negatively. HEART has nominal human unreliability table, standard generic tasks and error-producing condition table. Accordingly, experts have the option to choose proper generalised generic tasks and related error producing conditions from tables for any specific task instead of developing such items themselves. Moreover, it is a straightforward technique for solving and performing natural human reliability analysis cases thanks to the standard tables. However, the specific task sometimes cannot be fit with generic tasks in the table. It is more suitable for petrochemical and nuclear industries. It must be developed and changed for appropriate use in other fields.

Conversely, in this study, SLIM method is selected to determine the HEP values of the tasks related to ECDIS cybersecurity because of the advantages, such as applicability for specific tasks, usability in case of lack of data due to expert opinion and arrangement of the system safety level with PSF functions.

2.2. Process of the SLIM method

Kayisoglu et al. (2022) presented a flow diagram as shown in Figure 1 for the SLIM method in their study, which handles the HEP for bunkering operation in the maritime. Accordingly, the SLIM method is performed according to the process shown in Figure 1.

The benefits and advantages of the step-by-step SLIM roadmap are as follows (Kayisoglu et al., 2022). The problem statement step procures a perspective from the author while determining the PSFs for the tasks in the SLIM method. In addition to defining and explicating the tasks, experts must provide great perspective and systematic approaches when weighting and rating the PSFs for each tasks provided. Moreover, defined PSFs functionally help specify operational achievements and strategic and financial activities to achieve success in any operation or task. Although expert judgement includes subjectivity, experienced and skilled experts do possess enough knowledge for the considered tasks and procure high-level information to overcome inaccessible and restrictive data for the relevant scenario. The weighting of PSFs for a specific scenario provides an initial sight about the criticality of the performance factors for the success of an operation as a whole. Procuring an initial view for the success of an operation is one

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

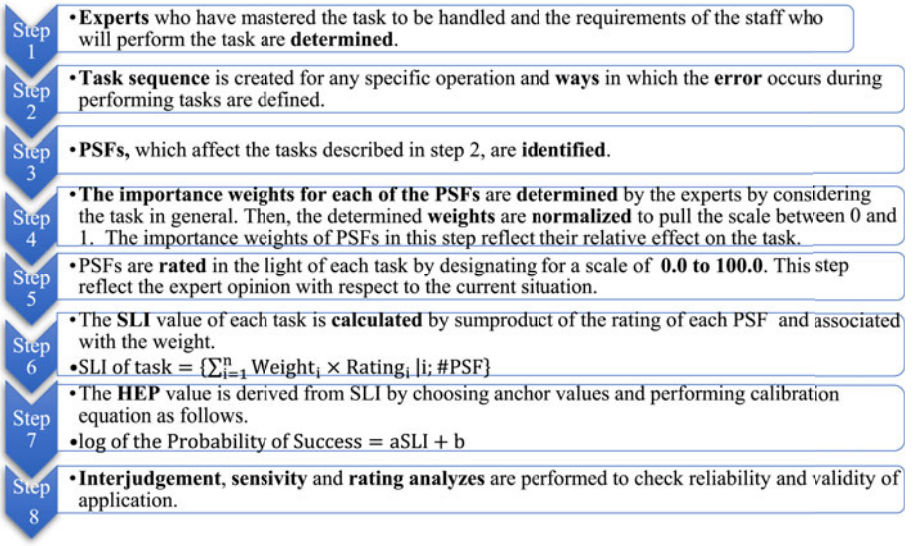

Figure 1. *Flow diagram for SLIM (Kayisoglu et al., 2022).*

of the advantages of the SLIM approach over other existing HRA methods. In the step of rating PSFs for each task, each task in an operation is evaluated specifically to define the steps where errors may occur. Hence, the risks related to the operation are systematically decreased by identifying strategic targets and taking required measures specific to each step. After achieving the SLI values and HEP values that are derived from SLI values, inter-judgement, sensitivity and rating analyses through analysis of variance (ANOVA) tests are carried out to check reliability and validity of the considered case study.

3. Case study on human error probability for ECDIS cyber security

3.1. Problem statement

As mentioned in the introduction, ECDIS is an electronic device that includes software, hardware, data and a human–machine interface. While ECDIS has a wide range of strengths for navigational officers in terms of design intent and functions, it also has a range of weaknesses, such as entry points that can be exploited by attackers across IT and OT configuration systems, communication interfaces with other cyber–physical systems onboard ships and human error. It is necessary to focus on the human aspect, especially navigating officers onboard a ship, when considering maritime cyber threats, as they interact with these systems and their vulnerabilities. Digital technologies must properly introduced on the bridge onboard a ship in a safe and efficient way, because if they are managed poorly, this can damage the safety of the ship and main root of maritime knowledge, skills and expertise. In this regard, the steps mentioned in the flow diagram of the SLIM in Figure 1 are followed and enforced to find human error probabilities for ECDIS cybersecurity specifically in this study.

3.2. Data collection

According to Figure 1, experts are identified according to having adequate and effective training, reasonable experience, and high level and related position on the considering tasks, scenarios or operation.

In this study, the considering tasks are related to the ECDIS operations pursued cybersecurity. These tasks are performed by navigation officers and controlled by a master mariner onboard. Five such experts evaluate the tasks and PSFs in this study. All of them are deck officers and masters onboard their ships.

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 3. *Demographic information of experts.*

EXPERTS	EXP1	EXP2	EXP3	EXP4	EXP5
Position	2nd Officer	Chief Officer	Chief Officer	2nd Officer	Master
Age	31	29	31	31	35
Sea experience (year)	24 month	40 month	38 month	30 month	60 month
Education level	MSc	BSc	Double BSc	BSc	BSc

According to the *International Convention on Standards of Training, Certification and Watch keeping for Seafarers* (STCW) (Safety4Sea, 2019), all our experts have to have taken qualified training and have at least one year of sea experience before becoming a deck officer; therefore these experts do have a high level experience in the sea as a deck officer or master. In addition, these experts are in key positions for performing ECDIS navigation practices on the bridge. In terms of ECDIS cybersecurity, as mentioned before, IMO introduced an amendment of MSC.428 resolution, which is 'Marine Cyber Risk Management in SMS onboard ships,' in 2017. Pursuant to this change, all ships must consider cybersecurity to be implemented in their SMS by 2021. For this reason, since 2017, shipping companies have to show the necessary care for the crew they have sent to their ships, especially the navigational officers and masters, to create an infrastructure on cybersecurity, because since the beginning of the 2021, all ships are inspected by the port state controls according to cybersecurity strategies stated in their SMSs. This is a regulatory indicator that masters and navigating officers should have cybersecurity awareness onboard ships.

Detailed demographic information about this study's experts is provided in Table 3. The reliability and validity of the obtained data and performed analysis are ensured in the reliability analysis section. According to the reliability analysis, the obtained data is reliable and applicable for the analysis.

For obtaining the weighting and rating of PSFs data that impacts ECDIS task cybersecurity, questionnaires were prepared with two sections. One section obtains expert rating scores of the PSFs in the view of considering each specific tasks about ECDIS cybersecurity. The other one obtains weights of the PSFs in view of the overall operation of ECDIS cybersecurity. The scoring of experts is performed by using a 1–9 point scale in both questionnaires, as SLIM requires (Embrey et al., 1984a, 1984b). The obtained data are firstly extended to 0–100 scale by multiplying 10 as requirements of the original SLIM, then used in equations standardised for SLIM in the following sections.

3.3. Tasks identification

According to the original SLIM, tasks or error modes related to operation are identified by discussion with a panel of experts, as well as by performing other steps of SLIM, such as identifying, weighting and rating PSFs as one panel (Embrey et al., 1984a, 1984b). However, in this study, the tasks related with ECDIS are determined by referencing the guide of operational handbook for ECDIS (Weintrit, 2009), and OCIMF's guide related to the recommendations on usage of ECDIS and preventing incidents (OCIMF, 2020). Then, these determined ECDIS tasks are integrated with the cybersecurity by referencing ECDIS cyber incidents (Svilicic et al., 2019a, 2019d, 2020; Karahalios, 2020; Kristic et al., 2021; Tam et al., 2022), various recommended international IT and OT cybersecurity standards for maritime such as *International Organization for Standardization* (ISO), IEC standards and NIST framework (ISO/IEC, 2010; BSI, 2011, 2017, 2018, 2021; Cichonski et al., 2012), and other codes of cybersecurity for ships (ICS and other organizations, 2016; Boyes and Isbell, 2017; IACS, 2020). Moreover, the developed final ECDIS tasks integrated with cybersecurity are checked by referencing a safety management manual of a shipping company, which is required by the IMO Maritime Safety Committee (MSC) according to the Resolution MSC.428(98) 'Maritime Cyber Risk Management in Safety Management Systems' (IMO, 2017a). The resolution requires that maritime cyber risks are appropriately considered in existing

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

safety management systems (as defined in the ISM Code), as of 1 January 2021. Although there are similar tasks on ECDIS cybersecurity in the safety management manual of the shipping company, as one example, it is understood that there is a need for further development of these manuals, which must be applied on ships with the additional tasks developed within the scope of this study. As a result, in Table 4, the ECDIS cybersecurity tasks are considered in four different specific categories: 'relationship between ECDIS manufacturers and navigating officers for ENC and ECDIS software update', 'responsibilities of navigating officers and company officers for ENC and ECDIS software updates', 'navigation responsibilities of deck officers on ECDIS' and 'company and vessel officers' awareness on cybersecurity technical requirements onboard'.

3.4. Identification of performance-shaping factors (PSFs)

The term 'performance-shaping factor' (PSF) stands for the items that impact the success of considered tasks or operation. In other words, PSFs provide information on preventing human errors/faults for any specific tasks or operation (Embrey et al., 1984a, 1984b). For identifying PSFs for ECDIS cybersecurity, this study used research in the literature, guidelines for ships cybersecurity, international IT and OT standards.

According to Kristic et al. (2021), for deck officers, ensuring the safety of the ship always takes precedence over meeting operational commitments and carrying out the ship's routine. In this context, their primary responsibility is navigation. Navigation onboard involves a range of several processes, which some of them are carried out in a specific order, some almost constantly, some randomly, and some rarely. The lack of established rules regarding the optimum use of navigation systems and techniques adds to the difficulty of this issue. Optimum use of navigation systems depends on the type of ship, the quality of navigational equipment on board, and the experience and skills of the seafarer (Bolat and Kayişoğlu, 2019).

At the same time, deck officers take the necessary measures to oversee all facilities of the procurement. For this purpose, they and other members on the bridge team ensure that they have appropriate training and preparedness for training and that all competence and systems are adequate. They should also ensure that all digital charts and publications are updated with the information provided by the Notice to Mariners (NtMs) and that all essential equipment is correctly outfitted. Since a ship has a dynamic lifecycle at sea and in ports, it is highly possible to make serious mistakes while performing a voyage plan. To plan a route carefully, the crew must use the necessary charts and monitor the ship's position for a comprehensive voyage, all of which are signs of a professional seafarer (ECE/TRANS/SC, 2013).

To ensure the safety of ships, any uncertainty about the location of the ship poses a hazard and should be cleared without delay. The best way to do this is by cross-checking data to avoid ambiguity around ship positions by utilizing all available tools and constantly controlling various sources of location information. The cross-checking method consists in using many different navigational techniques to maintain both operational controls and capabilities that may be required in an emergency situation. Any single navigational system creates a single point of failure; therefore, they must be backed up by another source to ensure the ship's safety (Nielsen, 2016).

On the other hand, Kristic et al. (2021) has highlighted the overreliance of the seafarer on ECDIS and the equipment it is tied to. Overreliance on ECDIS and other IT and OT assets create cyber-vulnerabilities in terms of human behaviour. The MSC has stated that unsecure tendencies of the seafarers, such as overreliance to technologic information onboard, is preventable not only training, but also with proper navigational culture, rigorous ships procedures, safety management rules, information sharing about related topics and awareness (IMO, 2017b).

All of the state-of-the-art guidelines, codes and regulations (ICS and other organizations, 2016; Boyes and Isbell, 2017; PaSea, 2018; National Cybersecurity Centre, 2020) mention that these navigation tasks are performed on ECDIS or other aids to navigation equipment by considering cybersecurity measurements. These measurements are required both technical measurements onboard

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 4. *Tasks for ECDIS cybersecurity.*

ECDIS Cybersecurity Operations	
T1	**Relationship between ECDIS Manufacturers and Navigating Officers for ENC and ECDIS Software Update**
1 · 1	Subsequent updates by ECDIS manufacturers are carried out only after appropriate testing, and there are release notes for masters and navigating officers to distinguish any changes.
1 · 2	If manufacturers detect any inconsistency in ECDIS performance, they issue technical bulletins to all ship owners/operators who manage ships equipped with their systems to highlight issues.
1 · 3	The manufacturers' technical bulletin includes mitigating measures for masters and navigating officers with future plans to correct the inconsistencies.
1 · 4	Ship owners/operators communicate with ECDIS manufacturers and ensure that relevant information is shared with ships under management immediately and acted upon with necessary mitigations according to Original Equipment Manufacturer (OEM) technical bulletins.
1 · 5	Any noted defect or inconsistency in ECDIS performance are promptly reported to the ECDIS manufacturer, with appropriate notices to Flag State Administrations or recognised organisation.
1 · 6	If Task 1 · 5 occurs, risk-assessed mitigations are implemented by the ship's crew until the defects have been corrected.
1 · 7	ECDIS manufacturers issue safety bulletins or software upgrades as soon as an error or inconsistency in ECDIS-related data or functionality is detected by a navigating officer. The operating system is updated with a security patch sent by the manufacturer.
1 · 8	Masters ensure that weekly updates to ENCs are properly set in all ECDIS stations by navigating officers according to the latest NMs.
T2	**Responsibilities of Navigating Officers and Company Officers for ENC and ECDIS Software Updates**
2 · 1	ECDIS ports for USB OR DVD drives are closed.
2 · 2	ENC updates are send by the manufacturer on a secure program, which should be a requirement in the whitelisting application of the ship or company.
2 · 3	If ECDIS ports are not closed, navigating officers should use unique and pre-scanned USB drives for receiving the ENC updates from the program and uploading them to the ECDIS.
2 · 4	The secure nature of the USBs used by navigating officers should be recorded in the whitelisting application of the ship or company. (Whitelisting has capability of defining the access control for portable storage devices, such as limiting documents to write, read and operate on removable medias; only on given permission for the use of encrypted devices and the use of drives with particular serial numbers.)
T3	**Navigation Responsibilities of Deck Officers on ECDIS**
3 · 1	Officers make and save the passage plan in ECDIS and ensure its availability, integrity and confidentiality by making sure there are no deletions, changes or lack of information in the passage plan.
3 · 2	Before assuming a navigational watch, the incoming officer positively confirms the ECDIS configuration against the passage plan requirements, such as safety settings, chart display and alarm system management. The outbound officer highlights all changes made to the ECIDS configuration, except for the passage plan parameters.
3 · 3	Officers use cross-checking methods to confirm the accuracy of information displayed on the ECDIS (e.g. RADAR or visual fix).

(*Continued.*)

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 4. *tcontinued.*

ECDIS Cybersecurity Operations	
3 · 4	Officers maintain the correct level of zoom on ECDIS to ensure safety critical information is displayed.
3 · 5	Following a cyber-attack and especially when approaching any waypoint or important area (e.g. canal, TSS, narrow channel, pilot station, etc), officers recheck the passage plan.
T4	**Company and Vessel Officers' Awareness on Cybersecurity Technical Requirements Onboard**
4.1	There is a defined shore-based Company Cybersecurity Officer who is responsible for all information security, including ECDIS.
4.2	There is a defined ship-based Cybersecurity Officer who is responsible for all information security, including ECDIS.
4.3	The contractual agreements between ships' officers and their employer state their and the companies' responsibilities for information security onboard.
4.4	All ship's officers (all ranks) are aware of their responsibilities and roles regarding cybersecurity policies and procedures onboard, including ECDIS.
4.5	There is routine training and drills around cybersecurity for ECDIS.
4.6	There are emergency plans for cyber-attacks for ECDIS.
4.7	Officers create a backup of ECDIS data at regular intervals to ensure navigational warnings, planned routes, manual ENC layers or other related information is recorded.
4.8	Officers are only be provided with access to the network and network services that they have been specifically authorised to use, including ECDIS.
4.9	Officers never connect to the internet on an ECDIS computer without appropriate security measures, such as a suitable firewall and anti-virus software.
4.10	Officers are aware that unauthorised access to network ports, protocols and services connected with ECDIS is prevented by setting a requirement for a login password.
4.11	Officers restrict access to software on the ECDIS computer, including the operating system, by password protection.
4.12	Officers understand any alarms or actions given by the system to detect, block and warn against cyber-attacks.
4.13	Officers are aware that remote and wireless access to ECDIS should be controlled by using an encryption key.
4.14	Officers set physical security zones and control access to the bridge (including access to ECDIS) to ensure that ECDIS is only used by trained and authorised personnel.
4.15	Officers do not remove any ECDIS equipment (including information and software) from the bridge or the ship without prior approval.
4.16	Officers make ensure about that there is availability continuously (emergency power supply, etc.) and integrity of ECDIS (monitoring of ECDIS).
4.17	Officers confirm removal of data and software licenses when any inconsistent equipment related to ECDIS (including storage media).

and having perception of the usage of these technical measurements. Accordingly, a cautious attitude about a potential cyber incident occurring suddenly, with the perception of cyber-attacks against ECDIS and other assets, engenders an attitude of waiting on alarm and good decision-making skills for safe navigation and secure systems. In addition, adequate time availability with these skills for error detection and correction also prevents human errors in the case of any cyber-attacks against ECDIS.

In the context of the references and after the controls by experts, the PSFs are specified as in Table 5.

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 5. *Performance shaping factors for ECDIS cybersecurity.*

PSFs	
PSF 1	Adequate ECDIS cyber-security training
PSF 2	Experience in cyber-attacks against ECDIS
PSF 3	Effective usage of ECDIS in compliance with good navigation practice
PSF 4	Awareness-Perception Knowledge of ECDIS cybersecurity
PSF 5	Not overly reliant on technology
PSF 6	Good navigation culture and behaviour integrated with cybersecurity
PSF 7	Safety Management System (SMS) – Safety Management Manual including detail professional prepared cybersecurity clauses, especially ECDIS cybersecurity
PSF 8	Policies, regulations and standards, checklist, code of practices related to ECDIS cybersecurity
PSF 9	ECDIS cybersecurity responsibilities
PSF 10	Appropriate safety culture (e.g. cyber incident reporting systems)
PSF 11	Cyber information sharing between persons, company, ship, maritime sector
PSF 12	A nervous (pessimistic) attitude about cyber-attacks against ECDIS (cyber-attack can be sudden and at any moment)
PSF 13	Adequate time available for error detection and correction
PSF 14	Effective decision-making skills
PSF 15	Technical security measures (e.g. software/ hardware, internet security systems, alarms of warning messages)

3.5. Weighting of PSFs

According to SLIM, after determining the tasks related to ECDIS cybersecurity and defining PSFs, experts weight the PSFs by considering which factor is more important to achieve the navigating officers the overall ECDIS cybersecurity tasks without any failure.

After experts give weighted PSFs scores of individually for the success of overall ECDIS cybersecurity tasks, according to the SLIM method, the arithmetic means of the individual weights for each PSFs and their normalised weights are calculated, as shown in Table 6. This step performed takes into consideration the process of aggregating the individual expert opinions to obtain an overall HEP value for each human task (Embrey et al., 1984b). The process requires that the arithmetic means of the individual weights and individual ratings of the PSFs are calculated and then used for gain an overall success likelihood index (SLI).

3.6. Rating of PSFs

Experts give scores for PSFs by taking each task into consideration separately. Like in Section 3.4, all individual expert ratings are extended to a scale of 0–100. After that, the arithmetic means of the individual experts' ratings are calculated for achieving the overall SLI, as in Table 7.

3.7. Calculation of success likelihood index (SLI)

According to SLIM (Embrey et al., 1984a, 1984b), the SLI values are obtained according to Equation (1) for each task:

$$\mathrm{SLI} = \left\{ \sum_{i=1}^{n} \mathrm{Weight}_i \times \mathrm{Rating}_i | i = \#\mathrm{PSF} \right\} \tag{1}$$

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 6. *Normalised weights.*

PSFs		Mean weighting scores	Normalised weighting scores
PSF 1	Adequate ECDIS cybersecurity training	82	0 · 073
PSF 2	Experience in cyber-attacks against ECDIS	78	0 · 070
PSF 3	Effective usage of ECDIS in compliance with good navigation practice	86	0 · 077
PSF 4	Awareness – Perception Knowledge of ECDIS cybersecurity	80	0 · 072
PSF 5	Not overly reliant on technology	48	0 · 043
PSF 6	Good navigation culture and behaviour integrated with cybersecurity	70	0 · 063
PSF 7	Safety Management System (SMS) – Safety Management Manual including detail professional prepared cybersecurity clauses, especially ECDIS cybersecurity	80	0 · 072
PSF 8	Policies, regulations and standards, checklist, code of practices related to ECDIS cybersecurity	74	0 · 066
PSF 9	ECDIS cybersecurity responsibilities	70	0 · 063
PSF 10	Appropriate safety culture (e.g. cyber incident reporting systems)	76	0 · 068
PSF 11	Cyber information sharing between persons, company, ship and maritime sector	80	0 · 072
PSF 12	A nervous (pessimistic) attitude about cyber-attacks against ECDIS (cyber-attack can be sudden and at any moment)	66	0 · 059
PSF 13	Adequate time available for error detection and correction	66	0 · 059
PSF 14	Effective decision-making skills	78	0 · 070
PSF 15	Technical security measures (e.g. software / hardware, internet security systems, alarms of warning messages)	82	0 · 073
Total		1,116	1 · 000

The resulting SLI values for each task are presented in Table 8. The multiplications of weight values with rating values (Weight × Rating) are demonstrated in the related column (see 'Product' column) in Table 8 for each task. In the last column, all product values for each task are summed up and SLI values for each task are achieved.

3.8. Transformation SLI to HEP

According to SLIM (Embrey et al., 1984a, 1984b), the HEP value is obtained by using SLI values and anchor values (a and b) corresponding to each task in accordance with the Equation (2):

$$\log \text{ of Probability of Success} = aSLI + b \tag{2}$$

The value obtained from Equation (2) represents the success probability of a considered task, and it is this value that allows us to determine the human error probability of each task. The value of success

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 7. *Means of PSFs ratings.*

Tasks		PSF 1	PSF 2	PSF 3	PSF 4	PSF 5	PSF 6	PSF 7	PSF 8	PSF 9	PSF 10	PSF 11	PSF 12	PSF 13	PSF 14	PSF 15
T1	1 · 1	78	60	56	70	26	64	78	76	60	72	80	52	70	56	82
	1 · 2	64	60	48	66	28	56	78	74	66	76	80	50	72	52	60
	1 · 3	62	60	52	70	38	64	76	78	70	68	76	50	60	58	58
	1 · 4	74	66	52	74	44	66	78	78	76	72	74	58	68	60	70
	1 · 5	78	68	64	76	38	62	78	78	66	72	82	58	70	64	70
	1 · 6	76	70	66	72	44	66	76	80	60	68	78	56	68	64	72
	1 · 7	68	64	62	70	40	62	70	74	64	66	76	56	62	56	70
	1 · 8	62	54	64	76	34	60	78	80	64	62	64	60	62	58	68
T2	2 · 1	82	64	60	74	36	72	78	78	76	68	72	66	62	64	72
	2 · 2	64	58	62	74	44	74	74	78	64	66	56	58	54	52	76
	2 · 3	80	66	60	88	44	78	84	82	80	80	70	78	54	64	78
	2 · 4	72	76	62	78	44	72	78	74	68	78	60	76	56	68	78
T3	3 · 1	76	78	68	78	46	76	76	72	70	80	56	78	54	68	76
	3 · 2	74	64	78	74	64	80	70	70	74	74	64	70	60	70	74
	3 · 3	72	74	76	82	66	78	82	72	66	70	60	66	54	68	78
	3 · 4	66	68	82	80	40	62	78	78	66	62	66	64	58	66	82
	3 · 5	76	64	74	78	56	76	78	78	72	64	64	74	64	70	76
T4	4 · 1	66	74	64	80	56	76	80	82	74	70	76	72	66	60	78
	4 · 2	68	74	68	78	58	76	82	82	74	72	78	74	62	64	78
	4 · 3	68	72	70	80	54	72	78	78	74	74	72	72	62	62	68
	4 · 4	80	72	66	82	50	70	82	84	74	74	72	74	62	64	72
	4 · 5	78	80	72	82	56	72	82	82	70	76	68	76	60	60	64
	4 · 6	76	78	70	82	58	68	80	82	70	68	76	70	60	68	68
	4 · 7	76	78	74	80	62	78	82	80	72	74	70	70	62	70	74
	4 · 8	72	70	78	78	54	68	76	76	68	66	72	70	58	56	76
	4 · 9	78	74	74	80	50	76	84	82	70	70	68	70	60	64	78
	4 · 10	78	74	72	80	52	68	82	82	70	68	72	74	58	64	78
	4 · 11	76	72	72	78	44	64	82	80	66	68	66	72	58	58	74
	4 · 12	76	70	72	74	50	70	82	80	70	66	70	68	62	60	82
	4 · 13	74	76	76	80	48	68	80	78	68	72	66	72	58	58	76
	4 · 14	74	72	76	80	54	72	84	82	74	68	66	72	56	66	78
	4 · 15	70	66	76	80	54	70	82	80	72	74	72	70	56	66	64
	4 · 16	70	74	80	78	56	74	78	80	70	72	66	64	60	68	76
	4 · 17	80	64	58	74	36	64	82	84	72	72	72	64	56	66	72

Table 8. *SLI values of tasks.*

Tasks		Product 1	Product 2	Product 3	Product 4	Product 5	Product 6	Product 7	Product 8	Product 9	Product 10	Product 11	Product 12	Product 13	Product 14	Product 15	SLI
T1	1·1	5·73	4·19	4·32	5·02	1·12	4·01	5·59	5·04	3·76	4·90	5·73	3·08	4·14	3·91	6·03	66·58
	1·2	4·70	4·19	3·70	4·73	1·20	3·51	5·59	4·91	4·14	5·18	5·73	2·96	4·26	3·63	4·41	62·85
	1·3	4·56	4·19	4·01	5·02	1·63	4·01	5·45	5·17	4·39	4·63	5·45	2·96	3·55	4·05	4·26	63·33
	1·4	5·44	4·61	4·01	5·30	1·89	4·14	5·59	5·17	4·77	4·90	5·30	3·43	4·02	4·19	5·14	67·92
	1·5	5·73	4·75	4·93	5·45	1·63	3·89	5·59	5·17	4·14	4·90	5·88	3·43	4·14	4·47	5·14	69·26
	1·6	5·58	4·89	5·09	5·16	1·89	4·14	5·45	5·30	3·76	4·63	5·59	3·31	4·02	4·47	5·29	68·59
	1·7	5·00	4·47	4·78	5·02	1·72	3·89	5·02	4·91	4·01	4·49	5·45	3·31	3·67	3·91	5·14	64·79
	1·8	4·56	3·77	4·93	5·45	1·46	3·76	5·59	5·30	4·01	4·22	4·59	3·55	3·67	4·05	5·00	63·92
T2	2·1	6·03	4·47	4·62	5·30	1·55	4·52	5·59	5·17	4·77	4·63	5·16	3·90	3·67	4·47	5·29	69·15
	2·2	4·70	4·05	4·78	5·30	1·89	4·64	5·30	5·17	4·01	4·49	4·01	3·43	3·19	3·63	5·58	64·22
	2·3	5·88	4·61	4·62	6·31	1·89	4·89	6·02	5·44	5·02	5·45	5·02	4·61	3·19	4·47	5·73	73·16
	2·4	5·29	5·31	4·78	5·59	1·89	4·52	5·59	4·91	4·27	5·31	4·30	4·49	3·31	4·75	5·73	70·05
T3	3·1	5·58	5·45	5·24	5·59	1·98	4·77	5·45	4·77	4·39	5·45	4·01	4·61	3·19	4·75	5·58	70·83
	3·2	5·44	4·47	6·01	5·30	2·75	5·02	5·02	4·64	4·64	5·04	4·59	4·14	3·55	4·89	5·44	70·94
	3·3	5·29	5·17	5·86	5·88	2·84	4·89	5·88	4·77	4·14	4·77	4·30	3·90	3·19	4·75	5·73	71·37
	3·4	4·85	4·75	6·32	5·73	1·72	3·89	5·59	5·17	4·14	4·22	4·73	3·78	3·43	4·61	6·03	68·97
	3·5	5·58	4·47	5·70	5·59	2·41	4·77	5·59	5·17	4·52	4·36	4·59	4·38	3·78	4·89	5·58	71·39
T4	4·1	4·85	5·17	4·93	5·73	2·41	4·77	5·73	5·44	4·64	4·77	5·45	4·26	3·90	4·19	5·73	71·98
	4·2	5·00	5·17	5·24	5·59	2·49	4·77	5·88	5·44	4·64	4·90	5·59	4·38	3·67	4·47	5·73	72·96
	4·3	5·00	5·03	5·39	5·73	2·32	4·52	5·59	5·17	4·64	5·04	5·16	4·26	3·67	4·33	5·00	70·86
	4·4	5·88	5·03	5·09	5·88	2·15	4·39	5·88	5·57	4·64	5·04	5·16	4·38	3·67	4·47	5·29	72·51
	4·5	5·73	5·59	5·55	5·88	2·41	4·52	5·88	5·44	4·39	5·18	4·87	4·49	3·55	4·19	4·70	72·37
	4·6	5·58	5·45	5·39	5·88	2·49	4·27	5·73	5·44	4·39	4·63	5·45	4·14	3·55	4·75	5·00	72·15
	4·7	5·58	5·45	5·70	5·73	2·67	4·89	5·88	5·30	4·52	5·04	5·02	4·14	3·67	4·89	5·44	73·92
	4·8	5·29	4·89	6·01	5·59	2·32	4·27	5·45	5·04	4·27	4·49	5·16	4·14	3·43	3·91	5·58	69·85
	4·9	5·73	5·17	5·70	5·73	2·15	4·77	6·02	5·44	4·39	4·77	4·87	4·14	3·55	4·47	5·73	72·64
	4·10	5·73	5·17	5·55	5·73	2·24	4·27	5·88	5·44	4·39	4·63	5·16	4·38	3·43	4·47	5·73	72·20
	4·11	5·58	5·03	5·55	5·59	1·89	4·01	5·88	5·30	4·14	4·63	4·73	4·26	3·43	4·05	5·44	69·53
	4·12	5·58	4·89	5·55	5·30	2·15	4·39	5·88	5·30	4·39	4·49	5·02	4·02	3·67	4·19	6·03	70·86
	4·13	5·44	5·31	5·86	5·73	2·06	4·27	5·73	5·17	4·27	4·90	4·73	4·26	3·43	4·05	5·58	70·80
	4·14	5·44	5·03	5·86	5·73	2·32	4·52	6·02	5·44	4·64	4·63	4·73	4·26	3·31	4·61	5·73	72·28
	4·15	5·14	4·61	5·86	5·73	2·32	4·39	5·88	5·30	4·52	5·04	5·16	4·14	3·31	4·61	4·70	70·73
	4·16	5·14	5·17	6·16	5·59	2·41	4·64	5·59	5·30	4·39	4·90	4·73	3·78	3·55	4·75	5·58	71·71
	4·17	5·88	4·47	4·47	5·30	1·55	4·01	5·88	5·57	4·52	4·90	5·16	3·78	3·31	4·61	5·29	68·72

Table 9. *Estimated HEP for the best and worst case of ECDIS cyber-security task categories.*

ECDIS Cybersecurity Task Categories		Estimated HEP for the Best Case	Estimated HEP for the Worst Case	'a' constant value	'b' constant value
T1	Relationship between ECDIS Manufacturers and Navigating Officers for ENC and ECDIS Software Updates	10^{-3}	10^{-2}	$0 \cdot 0009255$	$-0 \cdot 096910$
T2	Responsibilities of Navigating Officers and Company Officers for ENC and ECDIS Software Updates	10^{-3}	10^{-2}	$0 \cdot 002553$	$-0 \cdot 301030$
T3	Navigation Responsibilities of Deck Officers on ECDIS	10^{-5}	10^{-3}	$0 \cdot 001761$	$-0 \cdot 221849$
T4	Company and Vessel Officers' Awareness on Cybersecurity Technical Requirements Onboard	10^{-2}	10^{-1}	$0 \cdot 004260$	$-0 \cdot 522879$

probability should be subtracted from 1 after the anti-log of it is taken. The constant values of 'a' and 'b' in Equation (2) are the special items to SLIM and they are calculated by using SLIs of any two tasks related to considered operation and their HEP values, which have already been known or established before (Embrey et al., 1984a). For ECDIS cybersecurity, the two tasks, the HEP values of which are already known, are not encountered in the literature or from any risk assessment that have made by ships or in the shipping company. Hence, in this study, the absolute probability judgement method is used to find 'a' and 'b' endpoints for each of the four different task categories developed for ECDIS cybersecurity. The method of absolute probability judgement provides data for most rare-event operations or scenarios when the data frequency may not exist by the way of absolute probability judgments of experts on the best and worst cases for the evaluated operation (Kayisoglu et al., 2022).

In this study, experts focus on the four different categories of ECDIS cybersecurity and estimate the human error probability for the best and worst cases in these categories separately by taking into consideration the situation where PSFs are as bad as possible. These are the situations which navigating officers must have in order to successfully complete ECDIS cybersecurity missions, and vice versa. After obtaining HEP values of the two reference tasks for each task category thanks to the absolute probability judgement method, the values of 'a' and 'b'are found by using '0' and '100' values as SLI values in Equation (2) for the worst- and best-case scenarios, respectively. The obtained reference HEP values are supposed to be reasonable and reliable for the ECDIS cybersecurity tasks when trusting to experts' experience and knowledge as in all research sourced by expert opinion (Embrey et al., 1984a, 1984b; He et al., 2008; Hakam and Ratriwardhani, 2013) and examining the cyber incidents or attacks against ECDIS in literature. Estimated HEP values for best and worst cases regarding ECDIS cybersecurity and constant values derived from them are detailed in Table 9. In Table 10, unknown HEP values for evaluated tasks are obtained by using SLI values in Table 8 and 'a' and 'b' constant values in Table 9 in the Equation (2).

3.9. Reliability analyses

According to Embrey et al.'s sustainable method requirements, the reliability analyses of SLIM specifically include analysis of rating data, sensitivity analysis and inter-judge consistency analysis. These reliability analyses are carried out through the tests of two-way ANOVA by considering intended purposes (Embrey et al., 1984a).

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 10. *Human error probability for each tasks.*

Tasks		SLI	Log of Success Prob.	Success Prob.	HEP
T1	1 · 1	67	−0 · 0353	0 · 9219	0 · 0781
	1 · 2	63	−0 · 0387	0 · 9146	0 · 0854
	1 · 3	63	−0 · 0383	0 · 9156	0 · 0844
	1 · 4	68	−0 · 0341	0 · 9246	0 · 0754
	1 · 5	69	−0 · 0328	0 · 9272	0 · 0728
	1 · 6	69	−0 · 0334	0 · 9259	0 · 0741
	1 · 7	65	−0 · 0369	0 · 9184	0 · 0816
	1 · 8	64	−0 · 0378	0 · 9167	0 · 0833
T2	2 · 1	69	−0 · 1245	0 · 7507	0 · 2493
	2 · 2	64	−0 · 1371	0 · 7293	0 · 2707
	2 · 3	73	−0 · 1143	0 · 7687	0 · 2313
	2 · 4	70	−0 · 1222	0 · 7547	0 · 2453
T3	3 · 1	71	−0 · 0971	0 · 7996	0 · 2004
	3 · 2	71	−0 · 0969	0 · 8000	0 · 2000
	3 · 3	71	−0 · 0962	0 · 8014	0 · 1986
	3 · 4	69	−0 · 1004	0 · 7936	0 · 2064
	3 · 5	71	−0 · 0961	0 · 8014	0 · 1986
T4	4 · 1	72	−0 · 2163	0 · 6078	0 · 3922
	4 · 2	73	−0 · 2121	0 · 6136	0 · 3864
	4 · 3	71	−0 · 2211	0 · 6011	0 · 3989
	4 · 4	73	−0 · 2140	0 · 6109	0 · 3891
	4 · 5	72	−0 · 2146	0 · 6101	0 · 3899
	4 · 6	72	−0 · 2156	0 · 6088	0 · 3912
	4 · 7	74	−0 · 2080	0 · 6195	0 · 3805
	4 · 8	70	−0 · 2253	0 · 5952	0 · 4048
	4 · 9	73	−0 · 2134	0 · 6117	0 · 3883
	4 · 10	72	−0 · 2153	0 · 6091	0 · 3909
	4 · 11	70	−0 · 2267	0 · 5933	0 · 4067
	4 · 12	71	−0 · 2210	0 · 6011	0 · 3989
	4 · 13	71	−0 · 2213	0 · 6008	0 · 3992
	4 · 14	72	−0 · 2150	0 · 6095	0 · 3905
	4 · 15	71	−0 · 2216	0 · 6003	0 · 3997
	4 · 16	72	−0 · 2174	0 · 6062	0 · 3938
	4 · 17	69	−0 · 2302	0 · 5886	0 · 4114

The aim of the ANOVA tests is to compare the means of two groups or more. It is a collection of statistical models used to analyse differences between means and their correlated variation between and within groups. ANOVA is based on the law of total variance, in which the observed variance in a given variable is divided into components attributable to different sources of variation (Emerson, 2017). According to the ANOVA test, when the significance values (p) in ANOVA test results are less than 0 · 05, it means that considered dependent variable significantly differ between considered independent variables or groups (Gamage and Weerahandi, 1998).

In this study, for analysis of rating data, the intended purpose is that the PSF ratings significantly become different between PSF categories and evaluated tasks. With the sensitivity analysis, it is aimed that weight values significantly become different between PSF categories, but they do not significantly become different between tasks. For inter-judge consistency analysis, it is given that individual log HEP

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 11. *ANOVA results for inter-judge consistency.*

Tests of Between-Subjects Effects

Dependent Variable: Indiv_LOGHEP_Values

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	2·341[a]	2	1·170	290·512	0·000
Intercept	0·051	1	0·051	12·574	0·001
Task	2·333	1	2·333	579·149	0·000
Expert	0·008	1	0·008	1·875	0·173
Error	0·673	167	0·004		
Total	15·461	170			
Corrected Total	3·014	169			

[a]R Squared = 0·777 (Adjusted R Squared = 0·774).

values significantly become different between evaluated tasks, but they do not significantly become different between experts. If these purposes are confirmed by the analysis results, it is ensured that the obtained data for this study is valid and SLIM analysis results are reliable.

In this context, the results of ANOVA tests for each reliability analysis are presented in Tables 11–13. According to the inter-judge consistency analysis in Table 11, the results showed that individual log HEP values significantly become different between evaluated tasks ($p < 0 \cdot 05$) but they do not significantly become different between experts ($p > 0 \cdot 05$). The results of inter-judge consistency analysis are consistent with intended purpose in this study.

The interclass correlation coefficient, which states the mean correlation between the experts' opinions, is obtained via Equation (3). 'F' value in Equation (3) represents '*F*' value of Expert in Table 9 and '*n*' shows number of experts. The result of Equation (3) (0·998 – the closer it is to '1', the higher-level agreement between experts it is) evidences very high-level agreement between experts:

$$r = \frac{F - 1}{F + (n + 1)} = \frac{579 - 1}{579 + (5 + 1)} = 0 \cdot 988 \tag{3}$$

According to the sensitivity analysis in Table 12, weight values significantly become different between PSF categories ($p < 0 \cdot 05$) but they do not significantly become different between tasks ($p > 0 \cdot 05$). These results are in line with the desired expectations of this study. In addition, recommendations are designed in the findings and discussions by interrupting the weights of PSF categories to identify which PSFs have the greatest effect on the probability of success or failure about ECDIS cybersecurity. This is a significant advantage of SLIM over other approaches.

According to the rating analysis in Table 13, PSF ratings significantly become different between PSF categories and evaluated tasks ($p < 0 \cdot 05$). The result of rating analyses are consistent with the intended purpose in this study. Accordingly, the mean of the PSF ratings can be approved as a measure of the overall quality of the ECDIS cybersecurity with regard to the tasks under consideration.

In accordance with the results of the reliability analysis, the obtained data from experts for this study is valid and the results of SLIM analysis are reliable and commendable.

3.10. Findings and discussions

The results of SLIM analyses in Table 10, Figures 2 and 3 allow us better to understand the human error probabilities for ECDIS cybersecurity and the impact of PSFs on ECDIS cybersecurity, respectively.

Among the task categories considered for ECDIS cybersecurity the fourth category, which includes tasks related to company and vessel officers awareness on cybersecurity technical requirements onboard,

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

Table 12. *ANOVA results for sensitivity analysis.*

Tests of Between-Subjects Effects					
Dependent Variable: Weights					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	408 · 486[a]	2	204 · 243	2 · 461	0 · 086
Intercept	387,653 · 133	1	387,653 · 133	4,670 · 862	0 · 000
Task	0 · 000	1	0 · 000	0 · 000	1 · 000
PSFs	408 · 486	1	408 · 486	4 · 922	0 · 027
Error	42,077 · 914	507	82 · 994		
Total	2,865,520 · 000	510			
Corrected Total	42,486 · 400	509			

[a]R Squared = .010 (Adjusted R Squared = .006)

Table 13. *ANOVA results for rating analysis.*

Tests of Between-Subjects Effects					
Dependent Variable: ratings					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	2,202 · 320[a]	2	1,101 · 160	12 · 207	0 · 000
Intercept	303,287 · 037	1	303,287 · 037	3,362 · 227	0 · 000
PSFs	1,842 · 814	1	1,842 · 814	20 · 429	0 · 000
Task	359 · 506	1	359 · 506	3 · 985	0 · 046
Error	45,733 · 531	507	90 · 204		
Total	2,483,780 · 000	510			
Corrected Total	47,935 · 851	509			

[a]R Squared = .046 (Adjusted R Squared = .042)

has the highest possibility for failure. In this category, navigating officers mostly fall into error related to performing removal of data and software licenses or any inconsistent equipment related to ECDIS, including storage media. At the same time, all tasks in the fourth category involve very close failure probabilities. Regarding tasks in the fourth category, navigating officers should consciously restrict access to software on the ECDIS computer, including the operating system, by password protection for ensuring cybersecurity. Additionally, they should only be provided with access to the network and network services that they have been specifically authorised to use for ECDIS cybersecurity. They should not remove any ECDIS equipment (including information and software) from the bridge or the ship without prior approval. Finally, crew should be aware that remote and wireless access to ECDIS should be controlled by using an encryption protocols. These tasks include critical level of failure possibilities according to the analysis results. To prevent these failures, navigating officers should have and understand policies, regulations, standards, checklists and code of practices related to ECDIS cybersecurity, according to the analysis results as detailed in Table 7. Additionally, these technical security processes and procedures measures (e.g. software/hardware, internet security systems, alarms of warning messages) related to ECDIS cybersecurity should have a place in the Safety Management System (SMS) and Safety Management Manuals, including detailed professional prepared cybersecurity clauses, especially ECDIS cybersecurity. Essentially, navigating officers should have constant awareness

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

of ECDIS cybersecurity and then adequate ECDIS cybersecurity education and training in order to search and understand these process and procedures in the SMS and other sources and perform them onboard a ship in the scope of SMS.

In accordance with the analysis results, the second highest failure probabilities for ECDIS cybersecurity relates to the responsibilities of navigating officers and company officers to update ENC and ECDIS software . The most likely failure in this context is either ENC updates are not sent by the manufacturer on a secure program or this secure program does not address in the whitelisting application of the ship or company. Whitelisting has capability of defining the secure items, applications, network and access points, such as whitelisted access control for portable storage devices including limiting documents to write, read and operate on removable medias; only on given permission for the use of encrypted devices and the use of drives with particular serial numbers. For this reason, whitelisting is one important technical measures that should be established and adopted by companies to ensure all ship cybersecurity, including ECDIS. Then, unclosed ECDIS ports for external portable drives such as USB are also a highly possible failure onboard a ship. In addition to this, navigating officers generally do not use unique and pre-scanned USB drives for receiving the ENC updates from the program and uploading them to the ECDIS, and the USBs used by navigating officers are not to be recorded in the whitelisting application of the ship or company. Such mitigations are useful for tasks in the fourth category, for avoiding these failures. Firstly, the requirements related to closing of ECDIS ports should take place in SMS onboard a ship, and ENC and ECDIS software updates protocols and communications should be secured, which includes strategies such as whitelisting. If ECDIS ports are not closed, the requirement of usage of unique and pre-scanned USB drives recorded in the whitelisting application should be involved in SMS, as well. Navigating officers should have the adequate education to understand related technical measures and awareness of these requirements to provide ECDIS cybersecurity.

When evaluating the tasks in the third category, all tasks have a very similar probability of failure. This category consists of navigation responsibilities for navigating officers on ECDIS along with on the cybersecurity. After navigating officers make and save the passage plan in ECDIS, they do not generally ensure the availability, integrity and confidentiality of it by making sure no deletions, changes or lack of information can be made to the passage plan. Additionally, to understand the integrity of the passage plan, officers should maintain the correct level of zoom on ECDIS charts to ensure safety critical information is displayed on ECDIS. However, according to the results, this has one of the highest possible failure in this category. Moreover, before taking over a navigational watch, the incoming navigating officers generally error by not confirming the ECDIS configuration against the passage plan requirements, such as safety settings, chart display and alarm system management. The outbound officer does not highlight any changes made to the ECIDS configuration, which is except for the passage plan parameters, if there is one. Before that, they should use cross-checking methods with such as radar or visual fix to confirm the accuracy of information displayed on the ECDIS. However, although this task is a low-probability error in this category, it is still an important task that may not be performed and may affect other tasks. Finally, following a cyber-attack and especially when approaching any waypoint or important area (e.g. canal, TSS, narrow channel, pilot station, etc), officers can err by not rechecking the passage plan. According to these results, the most essential factors affecting these failures are effective usage of ECDIS in compliance with good navigation practice along with the perception knowledge of ECDIS cybersecurity. In this scope, navigating officers should have good navigation culture and behaviour integrated with cybersecurity and keep themselves on the alarm that cyber-attack can occur suddenly and at any moment.

Finally, among the task categories considered for ECDIS cybersecurity, the first category, which includes tasks related to relationship between ECDIS manufacturers and navigating officers for ENC and ECDIS software update, has the lowest possibility for failure. In this category, the highest possible failure is that if manufacturers detect any inconsistency in ECDIS performance, they do not generally issue technical bulletins with mitigating measures to all ship owners/operators who manage ships equipped with their systems to highlight issues and to correct inconsistencies. When this happens, the masters and navigating officers cannot be aware of the issues and cannot develop any protective measures for

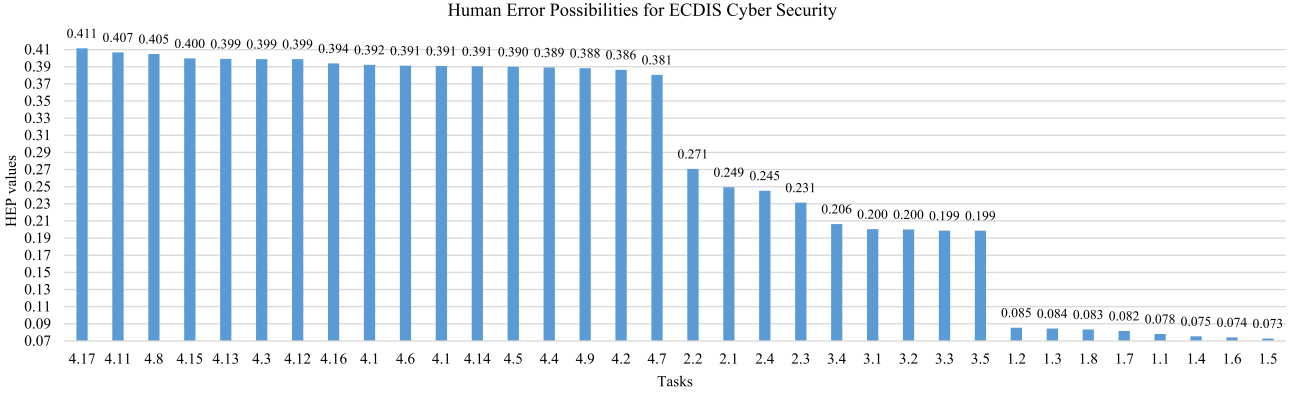

Figure 2. *HEP graph for ECDIS cybersecurity.*

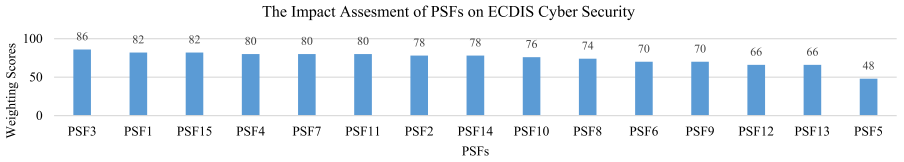

Figure 3. *The impact assessment of PSFs on ECDIS cybersecurity.*

future plans, and most importantly they cannot determine whether the technical issue is derived from a cyber-attack or not. This is followed by that a navigating officer not able to detect the future errors of ECDIS manufacturers' safety bulletins or software upgrades or future inconsistencies in ECDIS-related data or functionality the next time. To prevent these failures, it is recommended that cyber information-sharing policies between persons, company, ship and other stakeholders in the maritime sector, such as ECDIS manufacturers, should be developed and adopted by related parties and should be addressed in the SMS of shipping companies.

All in all, evaluating overall ECDIS cybersecurity, the most important factors to ensure effective cybersecurity for it are (i) effective usage of ECDIS in compliance with good navigation practice along with cybersecurity perception; (ii) adequate ECDIS cybersecurity training; (iii) developing technical security measures, and addressed them in safety management system of shipping companies; and (iv) developing cyber information sharing between related stakeholders in the maritime sector.

4. Conclusion

In maritime cybersecurity, several available policies and procedures, standards and guidelines only put forward frameworks for the physical, application, network, data security and requirements of usage aspects of security. They comprise essential components for entire maritime cybersecurity official strategies in terms of technical mitigations. However, the human factor is not always specified clearly as a part of defence strategies. We argue that the human factor and management of the associated human strengths and vulnerabilities should instead be fully incorporated and acknowledge the key components in sociotechnical systems in the maritime field, to create robust cybersecurity protection, prevention, organisational integrity and safety assurance.

In this study, the contributions on determining the human error probabilities related to ECDIS cybersecurity and on developing strategies for ECDIS cybersecurity onboard ships are presented to support this concept, and propose solutions based on the sociotechnical vulnerabilities identified.

The analysis results provides to enable practical anchorage to not only navigating officers for enhancing their perceptions of risks related to their responsibilities on ECDIS cybersecurity, but also to shipping company managers and ECDIS manufacturers for improving the design of safety critical systems and exist procedures for ECDIS cyber space. By considering the human reliability analysis results as the pre-emptive approaches, this study can provide an insight for industrial policies, guidelines and best practices in ECDIS cybersecurity risk management in terms of the behavioural and cultural aspects of shipping. More specifically, ship owners or managers can change available cyber policy, procedures and checklists in accordance with the International Safety Management (ISM) Code to improve effectiveness. This would form new ECDIS cybersecurity rules and crewmember roles and responsibilities. Accordingly, ship managers can develop effective drills and trainings about ECDIS cybersecurity tailored for crew members onboard ships which is in their service intended for measure the level of their own crews' human error possibilities and improve the critical level of human errors obtained in this study.

These results are relevant because human factors and poor processes cause an extensive part of security breaches in all sectors. If the sector ignores this, marine insurers are may struggle to improve the extensive scope of maritime cyber insurance specifically due to: (i) the unknown nature of cyber risk; (ii) lack of actuarial data; (iii) improving and changing continually technology; and (iv) uncertainties

https://doi.org/10.1017/S0373463322000534 Published online by Cambridge University Press

responsibilities and roles of related stakeholders such as crew members, managers or owners in the shipping companies for cyber spaces onboard a ship. If shipping companies owners or managers can specify the roles and responsibilities of crewmembers under the safety management system and manual, this also provides pivot points for marine insurers to define the claims in any case of cyber-attack, especially for ECDIS.

This study also demonstrated that ECDIS manufacturers should make further developments for engaging navigating officers onboard and shipping company managers in all elements of a process, such as publishing technical bulletins, updating operating systems of ECDIS and detecting any inconsistencies in ECDIS functionality. In addition, they can consider making familiarisation and orientation of ECDIS workstation for adding navigating officers' capabilities to ECDIS cybersecurity tasks by considering human errors in this study. These further developments requires in-depth knowledge of the technical aspect of cybersecurity and ECDIS technology. Therefore, in order to understand and apply the technical requirements of ECDIS cybersecurity, they should have well-designed education and training involving ECDIS dynamics, regulations, standards, policies, and law on the ECDIS cybersecurity, and responsibilities and liabilities for ECDIS cybersecurity. In addition, this study highlights that, currently, navigating officers onboard a ship should integrate their navigation skills and culture with the cybersecurity requirements and attitudes.

The insights obtained in this study help and to assist next-generation of responsible human factors for ECDIS cybersecurity in three key points: (i) they should be aware of ECDIS cyber risks, have adequate skills and qualifications for preventing these risks, be familiar with the procedures, levels of authorisation, and physical security barriers, and be well trained in risk response. They can be such as restricting access to network, software and operating system on the ECDIS by password protection, whitelisting, closing ECDIS ports for external portable drives, using pre-scanned USBs, integrating the navigational skills with cybersecurity perception, to be alert on for cyber-attacks and cross-checking navigational information received other cyber-physical system; (ii) SMSs and manuals, which are used to protect the operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard ships, should be re-designed to develop understanding and awareness of key aspects of cybersecurity, especially ECDIS cybersecurity, by considering points mentioned in (i) articles; (iii) marine insurers should take into consideration ECDIS cybersecurity responsibilities and liabilities of crew members as a checklist in order to identify claims of sides in any case of cyber-attack against ECDIS.

Acknowledgements. We would like to thank all participants for providing data.

Funding statement. This study is supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) - 2214-A – International Research Fellowship Programme for PhD Students [REF: 53325897-115.02-152823]. This study is also supported by University of Plymouth, Cyber-SHIP Lab.

Author contributions. The authors confirm contribution to the paper as follows: study conception and design: G. Kayisoglu, P. Bolat; data collection: G. Kayisoglu; analysis and interpretation of results: G. Kayisoglu, P. Bolat, K. Tam; draft manuscript preparation: G. Kayisoglu. All authors reviewed the results and approved the final version of the manuscript.

Competing interests. None.

References

Bolat, P. and Kayişoğlu, G. (2019). Antecedents and consequences of cybersecurity awareness: a case study for Turkish maritime sector. *Journal of Eta Maritime Science (JEMS)*, **7**(4), 44–360.

Boyes, H. and Isbell, R. (2017). Code of Practice: Cybersecurity for Ships. IET Standards, Department for Transport, and Defence Science & Technology Laboratory (UK).

BrčićSrđan, D., Žuškin, S., Valčic, S. and Francic, V. (2018). Implementation of the ECDIS System: AN OOW Perspective as an Integral Part of Educational Improvement. *IAMU 2018: Annual General Assembly (AGA) of the International Association of Maritime Universities (IAMU)*, 121–128.

BS EN IEC 61162-1. (1996). Maritime navigation and radiocommunication equipment and systems – Digital interfaces – BS EN IEC 61162-1-1996.

BS EN IEC 61162-2. (1999). Maritime navigation and radiocommunication equipment and systems – Digital interfaces – BS EN IEC 61162-2-1999.

BS EN IEC 61162-450. (2018). Maritime navigation and radiocommunication equipment and systems – Digital interfaces – BS EN IEC 61162-450:2018.

BS EN IEC 63154. (2021). Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results – BS EN IEC 63154:2021.

BS EN ISO-IEC 27001. (2017). Information technology – Security techniques-Information security management systems-Requirements – BS EN ISO-IEC 27001-2017.

BSI ISO-IEC 61162-460. (2018). Maritime navigation and radiocommunication equipment and systems – Digital interfaces – BS EN IEC 61162-460-2018+A1-2020.

BS ISO-IEC 27005. (2011). Information technology – Security techniques-Information security risk managemnet – BS ISO-IEC 27005-2011.

Calixto, E. (2016). Human reliability analysis. In *Gas and Oil Reliability Engineering*, pp. 471–552. Elsevier. doi:10.1016/B978-0-12-805427-7.00005-1

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer security incident handling guide : Recommendations of the national institute of standards and technology. *NIST Special Publication*, **800–61**, 79.

DNV-GL. (2016). Cybersecurity Resilience Management for Ships and Mobile Offshore Units in Operation. DNV-GL Corporate Report, DNVGL-RP-0(September), 1–86.

DNV-GL. (2022). The Cyber Priority. https://www.dnv.com/cybersecurity/cyber-insights/thecyberpriority.html (7 June 2022).

ECE/TRANS/SC. (2013). Recommendation on Electronic Chart Display and Information System for Inland Navigation (Inland ECDIS) (Issue Resolution No. 48-Revison 2).

Embrey, D. E., Humphreys, P., Rosa, E. A., Kirwan, B. and Rea, K. (1984a). SLIM-MAUD: an Approach to Assessing Human Error Probabilities Using Structured Expert Judgment. Volume I. Overview of SLIM-MAUD. In NUREG/CR-3518-Vol.1; BNL-NUREG-51716-Vol.1 ON: DE84012380.

Embrey, D. E., Humphreys, P., Rosa, E. A., Kirwan, B. and Rea, K. (1984b). SLIM-MAUD: an Approach to Assessing Human Error Probabilities Using Structured Expert Judgment. Volume II. Detailed analysis of the technical issues. Brookhaven National Lab., Upton, NY, USA.

Emerson, R. W. (2017). ANOVA and t-tests. *Journal of Visual Impairment and Blindness*, **111**(2), 193–196. doi:10.1177/0145482(1711100214

Evans, M., He, Y., Maglaras, L., Yevseyeva, I. and Janicke, H. (2019). Evaluating information security core human error causes IS-CHEC) technique in public sector and comparison with the private sector. *International Journal of Medical Informatics*, **127**, 109–119. doi:10.1016/j.ijmedinf.2019.04.019

Gamage, J. and Weerahandi, S. (1998). Size performance of some tests in one-way ANOVA. *Communications in Statistics Part B: Simulation and Computation*, **27**(3), 625–640. doi:10.1080/03610919808813500

Gunes, B., Kayisoglu, G. and Bolat, P. (2021). Cybersecurity risk assessment for seaports: a case study of a container port. *Computers and Security*, **103**), doi:10.1016/j.cose.2021.102196

Hakam, M. and Ratriwardhani, R. A. (2013). Identifikasi bahaya pada pekerjaan grinding di sebuah perusahaan manufaktur dengan menggunakan pendekatan succes likelihood index methode Indonesia. *Seminar Nasional Manajemen Teknologi* XIX, November, 1–8.

Hanzu-Pazara, R., Raicu, G. and Zagan, R. (2019). The impact of human behaviour on cybersecurity of the maritime systems. *Advanced Engineering Forum*, **34**, 267–274. doi:10.4028/www.scientific.net/aef.34.267

Hareide, O. S., Josok, O., Lund, M. S., Ostnes, R. and Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cybersecurity. *Journal of Navigation*, **71**(5), 1025–1039. doi:10.1017/S0373463318000164

He, X., Wang, Y., Shen, Z. and Huang, X. (2008). A simplified CREAM prospective quantification process and its application. *Reliability Engineering and System Safety*, **93**(2), 298–306. doi:10.1016/j.ress.2006.10.026

IACS. (2020). *Recommendation on Cyber Resilience*. International Association of Classification Societies, Recommendation No. 166, 1–57.

ICS and other organizations. (2016). *The Guidelines on Cybersecurity Onboard Ships*.

International Hydrographic Organization. (2017). *Information on IHO Standards related to ENC and ECDIS. Version 1.1*.

International Hydrographic Organization. (2018). *Current IHO ECDIS and ENC Standards*.

International Maritime Organization. (2009). MSC.282(86): *Adoption of Amendments to the International Convention for the Safety Of Life At Sea, 1974. Annex 1*.

International Maritime Organization. (2006). MSC.232(82): *Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS)*.

International Maritime Organization. (2017a). *Resolution MSC.1/Circ.1503/Rev.1, ECDIS – Guidance for Good Practice*.

International Maritime Organization. (2017b). *IMO Resolution MSC.428 (98)*. p. 428.

International Maritime Organization. (2017c). *Guidelines on Cyber Risk Management- . MSC-FAL 1/Circ.3*.

ISO/IEC. (2010). *International Standard ISO/IEC Information Technology – Security Techniques – Network Security – Threats, Design Techniques and Control - ISO/IEC 27033-3 (Vol. 2010)*.

Karahalios, H. (2020). Appraisal of a ship's cybersecurity efficiency: the case of piracy. *Journal of Transportation Security*, **13**(3–4), 179–201. doi:10.1007/s12198-020-00223-1

Kayisoglu, G., Gunes, B. and Besikci, E. B. (2022). SLIM based methodology for human error probability calculation of bunker spills in maritime operations. *Reliability Engineering and System Safety*, **217**, 108052. doi:10.1016/j.ress.2021.108052

Kristic, M., ŽuŁkin, S., Brčic, D. and Car, M. (2021). Overreliance on ECDIS technology: a challenge for safe navigation. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, **15**(2), 277–287. doi:10.12716/1001.15.02.02

Lagouvardou, S. (2018). *Maritime cybersecurity: concepts, problems and models*. Master thesis (issue July).

Larsen, M. H. and Lund, M. S. (2021). A maritime perspective on cyber risk perception: A systematic literature review. *IEEE Access*. doi: 10.1109/ACCESS.2021.3122433

Mraković, I. and Vojinović, R. (2019). Maritime cybersecurity analysis – how to reduce threats? *Transactions on Maritime Science*, **8**(1), 132–139. doi:10.7225/toms.v08.n01.013

National Cybersecurity Centre. (2020). *Cyber essentials: Requirements for IT infrastructure*. August, 1–12.

Nielsen, M. R. (2016). How A Ship´S Bridge Knows its Position – ECDIS Assisted Accidents From A Contemporary Human Factors Perspective. Lund University.

NIST. (2020). NIST Risk Managment Framework. In *Information Technology Laboratort Computer Security Resource Center*.

Norazahar, N. B. (2020). Human Factors Risk Assessment. In *Methods in Chemical Process Safety*, pp. 289–302. doi:10.1016/bs.mcps.2020.02.005

OCIMF. (2020). *Recommendations-on-Usage-of-ECDIS-and-Preventing-Incidents*, p. 32.

PaSea. (2018). Secure your Ecdis – prevent a cyber attack. DCP Circular 07-2018.

Pollock, T. (2017). Reducing Human Error in Cyber Security Using the Human Factors Analysis Classification System (HFACS). KSU *Proceedings on Cybersecurity Education, Research and Practice, Event 2*.

Pseftelis, T., Chondrokoukis, G. and Candidate, P. D. (2021). A study about the role of the human factor in maritime cybersecurity. *SPOUDAI Journal of Economics and Business*, **71**(1), 55–72.

Safety4Sea. (2019). *STCW Convention: General Requirements for Officers*. Maritime Knowledge, Seafarers. https://safety4sea.com/cm-stcw-convention-general-requirements-for-officers/

Svilicic, B., Brčić, D., Žuškin, S. and Kalebić, D. (2019a). Raising awareness on cybersecurity of ecdis. *TransNav*, **13**(1), 231–236. doi:10.12716/1001.13.01.24

Svilicic, B., Kamahara, J., Celic, J. and Bolmsten, J. (2019b). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, **18**(3), 509–520. doi:10.1007/s13437-019-00183-x

Svilicic, B., Rudan, I., Frančić, V. and Doričić, M. (2019c). Shipboard ECDIS cybersecurity: Third-party component threats. *Pomorstvo*, **33**(2), 176–180. doi:10.31217/p.33.2.7

Svilicic, B., Rudan, I., Jugović, A. and Zec, D. (2019d). A study on cybersecurity threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering*, **7**(10), 364. doi:10.3390/jmse7100364

Svilicic, B., Kristić, M., Žuškin, S. and Brčić, D. (2020). Paperless ship navigation: Cyber security weaknesses. *Journal of Transportation Security*, **13**(3–4), 203–214. doi:10.1007/s12198-020-00222-2

Tam, K. and Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, **3**(2), 147–164. doi:10.1080/23738871.2018.1513053

Tam, K. and Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, **18**(1), 129–163. doi:10.1007/s13437-019-00162-2

Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T. and Jones, K. (2022). Case study of a cyber-physical attack affecting port and ship operational safety. *Journal of Transportation Technologies*, **12**(01), 1–27. doi:10.4236/jtts.2022.121001

Tsimplis, M. and Papadas, S. (2019). Information technology in navigation: problems in legal implementation and liability. *Journal of Navigation*, **72**(04), 833–849. doi:10.1017/S0373463318001030

Version, D., Kujala, P. and Hirdaris, S. (2020). Prediction Model of Human Error Probability in Autonomous Cargo Ships. *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC)*,Vol. **2019**(2019), pp. 110–124. doi:10.2478/9788395669606-010

Vistiaho, P. (2017). *Maritime cybersecurity incident data reporting for autonomous ships*. Master thesis (issue November), Tampere University of Technology.

Weintrit, A. (2009). The electronic chart display and information system (ECDIS): An operational handbook. In *The Electronic Chart Display and Information System (*ECDIS*): AN Operational Handbook*. doi:10.1201/9781439847640

White Paper. (2022*). Human Affected Cybersecurity* (HACS) Framework. Chartered Institute of Ergonomics and Human Factors.

Cite this article: Kayisoglu G, Bolat P, Tam K (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *The Journal of Navigation* **75**: 6, 1364–1388. https://doi.org/10.1017/S0373463322000534