TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 18
Number 1
March 2024
DOI: 10.12716/1001.18.01.10

Cyber Risk Assessment for SHips (CRASH)

A. Oruc, G. Kavallieratos, V. Gkioulos & S. Katsikas
Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

ABSTRACT: The maritime industry is undergoing a digital transformation, with an increasing integration of Information Technology (IT) and Operational Technology (OT) systems on modern vessels. Its multiple benefits notwithstanding, this transformation brings with it increased cybersecurity risks, that need to be identified, assessed, and managed. Although several cyber risk assessment methodologies are available in the literature, they may be challenging for experts with a maritime background to use. In this paper we propose a simple and effective cyber risk assessment methodology, named Cyber Risk Assessment for SHips (CRASH), that can be easily implemented by maritime professionals. To showcase its workings, we assessed 24 cyber risks of the Integrated Navigation System (INS) using CRASH and we validated the method by comparing its results to those of another method and by means of interviews with experts in the maritime sector. CRASH can aid shipping companies in effectively assessing cyber risks as a step towards selecting and implementing necessary measures to enhance the cyber security of cyber-physical systems onboard their vessels.

1 INTRODUCTION

Given that approximately 80% of world trade by volume is carried out by vessels, sea transportation has a privileged place compared to other transportation modes [48]. The maritime sector has for some time been actively engaged with the digitalization of both shore and onboard systems and operations, leading to the digitally transformed shipping industry, also called "Shipping 4.0" [25].

Its multiple benefits notwithstanding, this transformation brings with it increased cybersecurity risks. Several cyber attacks have occurred in the maritime industry, and some of them have been suspected to be state-sponsored [37]. For example, in 2019, it was reported that 1,311 civilian ships were affected by Global Navigation Satellite System (GNSS) spoofing attacks between 2016 and 2018 [10]. In April 2016, a Global Positioning System (GPS) jamming attack impacted around 280 vessels off the coast of South Korea [14]. In June 2017, more than 20 vessels were exposed to a GPS jamming attack in the Black Sea [13]. In February 2017, malicious actors took control of the navigation system of an 8,250 TEU container vessels en route from Cyprus to Djibouti for 10 hours [8]. In April 2017, a modern U.S. destroyer had all its RAdio Detection And Ranging (RADAR) sets disabled by a Russian jet (Su-24) [34]. Additionally, the Electronic Chart Display and Information System (ECDIS) on a dry bulk vessel was infected with malware, resulting in financial losses due to delays in sailing and in ECDIS repair costs [7]. In another case, the power management system and administrative network of two different ships were infected with malware via a USB flash drive [7]. A more comprehensive account is given by Meland et

al., who discuss 46 maritime cyber incidents that occurred between 2010 and 2020 [32].

In light of these findings, of the increased financial value of the sector [27], and of the multitude of potential attackers, including such with advanced capabilities, the promotion of cyber security and safety of the maritime ecosystem becomes very important. Maritime is a highly standardized sectors, and maritime functions and operations are governed by corresponding standards and regulations. In 2017, the IMO published a circular to promote safe and secure shipping against cyber risks [23]. According to the circular, maritime companies must address cyber risks in their Safety Management System (SMS) by 01 January 2021. As of 02 January 2021, this requirement started to be verified in the Document of Compliance (DOC) audits of maritime companies. The International Electrotechnical Commission (IEC) published a standard in 2021 to specify requirements, testing methods, and required test results against cyber incidents for shipborne navigational components, shipborne radio equipment forming part of the Global Maritime Distress and Safety System (GMDSS), shipborne navigational aids, and Aids to Navigation (AtoN) [19].

The first step towards strengthening the cyber security and resilience of an ecosystem is to understand, analyze, and manage the cyber risks that it faces. Several cyber risk assessment methodologies are available in the literature, some of them specifically adapted to fit the needs of risk assessments in Cyber Physical Systems (CPS), such as those found onboard vessels. However, they may be challenging to use for experts with a maritime rather than a cybersecurity background. It must be noted that the involvement of sector experts in and their engagement with the assessment of cyber risks is paramount to obtaining accurate results. Note also that statistical data regarding cyber incidents in maritime is not available in the literature and various risk assessment methods make certain assumptions, regarding likelihood of occurrence, cost, and malicious actors. Therefore, their results depend heavily on expert judgement. To the best of our knowledge, a method that is easy for maritime domain experts to employ whilst also minimizing subjectivity, is yet to be proposed.

In this paper we propose such a simple and effective cyber risk assessment method, named Cyber Risk Assessment for SHips (CRASH), that can be easily applied by maritime professionals. CRASH was designed to reduce the need for expert judgements in the cyber risk assessment process for marine systems. CRASH employs unveiled cyber threats and vulnerabilities in the literature, previous cyber incidents and shipborne system architectures, to assess cyber risks.

The remaining of the paper is organized as follows: Section 2 presents a review of the related literature. The CRASH method is presented in section 3. Section 4 showcases the workings of CRASH by applying it to assess cyber risks of the INS. In section 5, we present the methodology for verifying CRASH and the results of applying it. Finally, section 6 offers a summary and recommends some possible future research directions.

2 RELATED WORK

Several risk assessment methods have been proposed in the literature, including [47, 2, 28, 1, 17, 4, 31] and several cyber risk assessments by using diverse methods, including Fine-Kinney, Attack Tree, STRIDE, and DREAD, have been carried out both for conventional vessels and autonomous ships [24, 25, 26, 38, 42, 44]. Moreover, works proposing novel risk assessment methods against cyber risks onboard ships have also appeared in the literature [9, 33, 46]. A guideline [24] published by iTrust presents potential cyber risks and mitigation measures for communication, navigation, cargo management, propulsion machinery, and power control systems. Svilicic et al. [44] present a risk assessment for the ECDIS on a training vessel. Shang et al. [42] offered a cyber risk assessment method and applied it to a cyber risk scenario of the ship control system. Kavallieratos et al. [25, 26] adapted and applied well-established methods, namely STRIDE and DREAD, to assess the cyber risks of CPSs onboard autonomous ships. Another method for assessing cyber risks at sea is CYber-Risk Assessment for Marine Systems (CYRA-MS), proposed by Bolbot et al. [9].

Cyber security risk is associated with the potential that threats will exploit vulnerabilities of an asset or group of assets and thereby cause harm to an organization. Cyber risk is assessed in terms of the likelihood of a threat occurring, the extent of the vulnerabilities to the threat, and the magnitude of the impact should the threat materialize; these constitute the elements of cyber risk. However, other choices for the elements of risk are possible. The SEP method [47] considers Severity, Exposure, and Probability as elements of risk. Severity describes potential consequences, such as occupational illness, injury, and death. Exposure reflects the required resources for a consequence, such as the amount of time, number of cycles, and number of people. Probability is defined as the likelihood of a consequence occurring. Severity and Probability assume values in the [1, 5] range, while the value of Exposure ranges in [1, 4]. The overall risk is calculated as the product of all three values. The Failure Modes and Effects Analysis (FMEA) method [2] assesses the failure risk of a component or system. Like SEP, it also assumes three elements of risk, namely Severity, Occurrence, and Detection. Occurrence is the likelihood of failure. Severity reflects the severity of a consequence, and Detection represents the detectability of a potential failure. Scores for each element range between 1 and 5, and the overall risk score -called Risk Priority Number (RPN)- is calculated by multiplying the three element scores. The Fine-Kinney method [28] also assumes three risk elements, namely Consequence, Likelihood, and Exposure. Consequence reflects undesirable incidents such as minor first-aid accidents, serious injuries, disabilities, and fatalities. Likelihood measures the possibility of a consequence, and Exposure reflects the frequency (e.g., daily, weekly, and monthly) of a potential consequence. Consequence is scored between 1 and 100, Likelihood between 0.1 and 10, and Exposure between 0.5 to 10. The risk level is determined by multiplying these scores. All these methods are quantitative and use a linear combination of the values of the risk elements

to calculate the overall risk score. While SEP and Fine-Kinney are used for safety risk assessments, FMEA is mostly used for the risk assessment of failures. A combination of FMEA and Fine-Kinney with fuzzy set theory is also available in the literature [1, 17].

3 CRASH: CYBER RISK ASSESSMENT FOR SHIPS

Several studies in the literature estimate risk levels by considering a combination of safety, financial, environmental, or reputation impact. However, each impact type may result in a different risk level. Therefore, assessing impacts individually would result in a more accurate risk assessment, as shown in [16]. The CRASH approach focuses only on the safety impact of cyber attacks against components and systems onboard ships. In this study, safety impact refers to the occurrence of a situation that may lead to a marine accident causing harm to people or the environment [36]. Potential consequences other than safety, such as financial, environmental, or reputation, are beyond the scope of the method. Risk management, including risk mitigation measures and reassessing risks, is also outside the scope.

3.1 *Elements of risk*

CRASH assumes three elements of risk, namely Severity, Probability, and Criticality. These are discussed in detail in subsequent sections. The overall cyber risk is calculated according to equation 1. The correspondence between numerical risk scores and qualitative risk levels in CRASH is depicted in Tab 1.

$$Risk = Severity\ (S) \times Probability\ (P) \times Criticality\ (C) \quad (1)$$

Table 1. Risk level in CRASH

Risk Score	Risk Level
1 - 20	Low
21 - 40	Medium
41 - 60	High

3.1.1 *Severity*

Severity is a measure of the impact caused by a cyber attack against systems onboard a ship. Two distinct flows are distinguished in marine systems, namely information flows and control flows. Both information and control signals may suffer from loss or manipulation. Loss refers to potential damages to availability and manipulation refers to potential damages to integrity. In assessing the severity value, several aspects should be considered, as discussed below.

The criticality of each information and control signal depends on the functions and operations that the signal is being used by. For instance, the position of own ship is more critical compared to the volume control or volume information of a GPS receiver. Further, the importance level varies under different threat scenarios. Accordingly, many factors such as ship type, position, weather and sea conditions, etc. should be considered during a cyber risk assessment. In the CRASH approach, the expert should determine whether the loss/manipulation of control or information is critical or not for ship operations. Manipulation of control/information is more dangerous than the loss of control/information at the same criticality level because it is more difficult to detect by seafarers or systems onboard ships. For instance, GPS spoofing (manipulation of information) [6] is riskier than GPS jamming (loss of information) [15] because it is harder to detect by the Officer On Watch (OOW) [18]. Loss/manipulation of information can be observed during an operation. However, loss/manipulation of control is noticed only when the control is required. Undoubtedly, both information and control could be critical for ship safety operations. However, particularly in case of an emergency, control is typically more important because of the time constraint to take action.

According to the International Safety Management (ISM) Code, "The Company should identify equipment and technical systems, the sudden operational failure of which may result in hazardous situations" [20]. The Oil Companies International Marine Forum (OCIMF) has classified hazardous situations as follows [36]:

- loss of steering;
- loss of propulsion;
- loss of power;
- loss of inert gas system;
- loss of gas monitoring system;
- loss of cargo/ballasting monitoring equipment;
- loss of mooring.

According to the OCIMF, loss of the stated functions may cause a marine casualty, which may harm people and/or the environment [36]. Accordingly, a potential cyber attack which may cause loss of such functions is considered to be a hazardous situation and it is assessed as having the highest severity level.

Based on the above reasoning, the matrix shown in Figure 1 results.

Score		1	2	
	Factor	loss	manipulation	
1	information	1	2	Situation
2	control	2	4	
3	critical information	3	6	
4	critical control	4	8	
		Hazardous		

Figure 1. CRASH severity levels.

The value of the severity element in CRASH is determined as shown in Table 2. Some risks may have multiple safety impact, for example both "minor - loss of information" and "severe - manipulation of a critical control". In such cases, severity is assigned the highest value, following the worst-case scenario approach.

Table 2. Severity Table

Class	Impact	Score
none	no safety impact	1
minor	loss of information, loss of control, manipulation of information	2
significant	loss of critical information, manipulation of control, loss of critical control	3
severe	manipulation of critical control, manipulation of critical information	4
catastrophic	hazardous situation	5

3.1.2 *Probability*

Probability measures the likelihood that a threat exploits a vulnerability or a set of vulnerabilities [41]. As there is very limited statistics of cyber incidents in the maritime industry, a purely quantitative approach to determining the likelihood is not possible. Instead, CRASH assumes four levels of such likelihood, namely None, that denotes a virtually impossible attack; Unlikely, that denotes the existence of possible scenarios; Possible, that reflects cases whose possibility of occurrence has been verified by experimental research; and Likely that reflects cases of cyber incidents that have actually occurred in the real world. Table 3 depicts the value of the probability element that CRASH assigns. If more than one option exists (e.g. both "occurred cyber incident" and "experimental research result"), the higher value is assigned.

Table 3. Probability Table

Class	Description	Score
none	virtually impossible	1
unlikely	scenario	2
possible	experimental research result	3
likely	occurred cyber incident	4

3.1.3 *Criticality*

Criticality measures the dependence on information or systems to achieve necessary functions and operations [35]. The value of criticality depends on two factors: redundancy and dependency. Redundancy denotes the existence of a backup system or component, while dependency denotes that a component requires another component to run reliably. Additionally, some components may be required to be connected to another component due to IMO requirements.

In case of a cyber attack against a component, the dependent components would be affected negatively. Accordingly, dependency is significant in terms of chain impact. Redundancy is an essential mitigation measure against cyber attacks as well as against failures. Critical systems on board ships must be equipped with redundant components. For instance, the steering system in the bridge might be out of order because of a failure. In such a case, the rudder of the vessel can be steered from the steering room (i.e., the emergency steering system).

The value of the criticality component in CRASH is determined by considering the Criticality Matrix depicted in Table 4. Redundancy may take on one of three values: available, partly, or unavailable. Unavailable denotes no redundant component; Available denotes that an alternative component that can carry out exactly the same function is available onboard the ship; and partly denotes that an alternative component that can carry out a similar function is available onboard the ship. Three values for dependency are assumed: No dependent component, One dependent component or More than one dependent components for the hazardous situations (discussed in section 3.1.1). For transforming the qualitative values in the table to numeric values, low criticality is scored 1, medium criticality is scored 2, and high criticality is scored 3.

Table 4. Criticality Matrix

	Dependency		
Redundancy	No Dependent Component	One Dependent Component	More than one dependent Components
Available	Low (1)	Low (1)	Medium (2)
Partly	Low (1)	Medium (2)	High (3)
Unavailable	Medium (2)	High (3)	High (3)

Table 5. Components of INS and their Redundancy

Component	Redundant	Result
AIS	N/A	Unavailable
Anemometer	N/A	Unavailable
BNWAS	N/A	Unavailable
Central Alert Management HMI	MFD	Available
Controls for M/E	Local controls in engine room (on M/E or in ECR)	Available
Controls for main rudder	Local controls in steering room	Available
Controls for thruster	Local controls in thruster room	Available
ECDIS	Back-Up ECDIS	Available
Echo Sounder	2nd Echo sounder	Available
GPS	2nd GPS	Available
Gyro-Compass	2nd Gyro compass	Available
HCS	N/A	Unavailable
Indicators	on local units	Available
Magnetic Compass	Gyro compass	Partly
MFD	Other MFDs	Available
NAVTEX	N/A	Unavailable
RADAR	If X band RADAR fails, S band can be used. If S band RADAR fails, X band can be used.	Partly
Rate of Turn Indicator (ROTI)	ROT calculation based on GPS	Partly
Rudder pump selector switch	Local controls in ECR or steering room	Available
Sound reception system N/A	Unavailable	
Speed and Distance Measuring Equipment (SDME)	Speed Over Ground (SOG) based on GPS	Partly
Steering mode selector switch	Steering mode selector switch in wings	Available
Steering position selector switch	N/A	Unavailable
TCS	N/A	Unavailable
Transmitting Heading Device	N/A	Unavailable

4 USE CASE: APPLYING CRASH TO THE INS

Modern vessels are equipped with various computerized systems serving different purposes, including navigation, propulsion, communication, cargo handling, safety, and security. Undoubtedly, the INS is one of the most critical systems onboard ships. The INS supports the OOW for safe navigation, by receiving data from several components, combining them, and providing timely alerts regarding dangerous situations at sea, such as geographic, traffic, and environmental hazards, or system failures [22]. The INS consists of several compulsory and elective components, including the Automatic Identification System (AIS), the GNSS, the Multifunctional Display (MFD), the RADAR, and the ECDIS. Several studies revealed the cyber threats and vulnerabilities of such components as well as of the INS as a whole [5, 6, 29]. Several cyber incidents targeted INS and its vulnerabilities have been extensively analyzed in the literature [39, 43, 30, 29]. Accordingly, the INS was selected to illustrate the workings of CRASH.

The application was performed in nine steps, as follows:

- Step 1: identification of the system and components;
- Step 2: identification of cyber risks;
- Step 3: identification of the redundancies;
- Step 4: identification of the dependencies;
- Step 5: determination of the severity;
- Step 6: determination of the probability;
- Step 7: determination of the criticality;
- Step 8: calculation of the risk score;
- Step 9: analysis of risks.

4.1 *Step 1: Identification of the System and Components*

The INS comprises 25 different components for different purposes, such as determining the heading, position, or speed [40]. Such components are listed in Table 5.

4.2 *Step 2: Identification of Cyber Risks*

The cyber risks of components are identified by means of a literature review. Not only academic papers but also other sources, such as websites, magazines, white papers, and guidelines, are scanned to find additional cyber threats, vulnerabilities, and incidents. Furthermore, additional cyber attack scenarios can be designed. Identified cyber risks for the INS are given in Table 6. Risks #1-18 in the table are based on findings in the scientific literature and in publicly available resources. Risks #19-24 correspond to potential risk scenarios. According to Table 6, eight INS components are exposed to cyber risks, namely the AIS, the Bridge Navigational Watch & Alarm System (BNWAS), the control for the main engine (M/E) (i.e., revolutions per minute (rpm) controller), the ECDIS, the GPS, the indicator (i.e., the indicator for starting air pressure), the MFD, and the RADAR.

Table 6. Cyber Risks of the INS

ID	Component	Risk
1	AIS	Ship spoofing (Receiving message belonging to fake vessels)
2	AIS	AtoN spoofing
3	AIS	Collision (i.e., Closest Point of Approach (CPA)) spoofing
4	AIS	AIS-SART spoofing (Receiving fake AIS-SART alert)
5	AIS	Weather forecasting
6	AIS	Altering Estimated Time of Arrival (ETA) of own vessel (AIS hijacking)
7	AIS	Frequency hopping attack
8	AIS	Timing attack
9	GPS	Jamming
10	GPS	Spoofing
11	RADAR	Eliminating RADAR targets
12	RADAR	Changing the position of the vessel in the RADAR display
13	RADAR	Out of order because of malware infection
14	RADAR	Jamming
15	ECDIS	Manipulation of the ship's position because of malware infection
16	ECDIS	Out of order because of malware infection
17	ECDIS	Modification of charts of ECDIS
18	Unknown	Loss of steering function
19	RADAR	Blocking change of RADAR range
20	AIS	Hiding the destination of other vessels
21	Controls for M/E	Blocking change of rpm for a Fixed-Pitch Propeller (FPP) vessel
22	Indicator	Manipulation of starting air pressure
23	BNWAS	Turning off by crew (internal cyber attack)
24	MFD	Disabling critical functions crew of all MFDs (internal cyber attack)

4.3 *Step 3: Identification of the Redundancies*

The third step involved identifying the redundant components for the eight components identified in step 2. The redundancy of each component was analyzed based on whether it would be affected by the same attack simultaneously or not. For example, a RADAR unit has a redundant RADAR unit, but during a RADAR jamming attack, both RADARs would be affected [34]. Thus, for Risks #11,12,13, and 19, the redundancy value for RADAR risks was determined as "partly", while for Risk #14, it was determined as "unavailable". It should be noted that the compromised component for Risk #18 is unknown, but the cyber attack resulted in the loss of steering. Therefore, the emergency steering system for Risk #18 was assumed to be a redundant system. The redundancy status by cyber risks is presented in Table 7.

4.4 *Step 4: Identification of the Dependencies*

All possible dependencies between the components of an INS as per the IMO requirements have been analyzed in [40]. However, in this study, the simplified dependencies shown in Table 8 are considered. In this table, the symbol "→" stands for depends between components. The GPS and the gyro compass are the most critical components in terms of dependency, as five components depend on the GPS and five components depend on the gyro compass.

The components under study are the AIS, BNWAS, control for M/E, ECDIS, GPS, indicator, MFD, and RADAR as shown in Table 6. The components that depend solely on the AIS or the GPS among compromised components are available, as shown in Table 9. Risk #18 is a hazardous situation. The number of dependent components is identified as "more than one dependent component", as mentioned in section 3.1.3.

Table 7. Redundancy by Cyber Risks

ID	Component	Result
1-8	AIS	Unavailable
9,10	GPS	Unavailable
11-13	RADAR	Partly
14	RADAR	Unavailable
15-17	ECDIS	Available
18	Unknown	Available
19	RADAR	Partly
20	AIS	Unavailable
21	Control for M/E	Available
22	Indicator	Available
23	BNWAS	Unavailable
24	MFD	Unavailable

Table 8. Simplified Dependencies of an INS

Component	AIS	GPS	Gyro Compass	Magnetic Compass	ROTI	SDME
AIS		→	→		→	
ECDIS		→	→			→
Gyro Compass		→				
HCS			→			→
RADAR	→	→	→			→
TCS		→	→			→
THD				→		
Total	1	5	5	1	1	4

4.5 *Step 5: Determination of the Severity*

The severity value of each of the identified risks was determined as described in Section 3.1.1. Two risks were assessed as "Catastrophic", four as "Minor", eight as "Significant", and ten as "Severe". The loss of steering function and the blocking of the change of M/E rpm were both classified as "Catastrophic" risks.

4.6 *Determination of the Probability*

The value of the probability of each risk was determined as described in Section 3.1.2. No risk probability was valued as "None". Risks #1, #9, and #10 have not only been observed in research experiments, they have also occurred in real-world cyber incidents. Therefore, these risks were considered to be of higher probability (i.e., "Likely"). The values of the probability element of all identified cyber risks are presented in Table 11, with six valued as "Likely", six as "Unlikely", and 12 as "Possible".

4.7 *Determination of the Criticality*

The criticality values were determined as described in Section 3.1.3. Both redundancies (discussed in Section 4.3) and dependencies (discussed in Section 4.4) were taken into account when determining the criticality of each component, as shown in Table 12.

4.8 *Calculation of the Risk Score*

The numeric risk scores are calculated using equation 1. The qualitative risk levels are determined by using Table 1 and are shown in Table 13.

Table 9. Dependency Table of Compromised Components

Dependent Components	Compromised Components A	B	C	E	G	I	M	R
AIS					→			
ECDIS					→			
Gyro Compass					→			
RADAR	→				→			
TCS					→			
Total	1	0	0	0	5	0	0	0

A- AIS; B- BNWAS, C- Control for M/E, E - ECDIS, G - GPS, I- Indicator, M- MFD, R- RADAR

Table 10. Severity values

ID	Definition	Class	Score
1	manipulation of critical information	severe	4
2	manipulation of critical information	severe	4
3	manipulation of critical information	severe	4
4	manipulation of information	minor	2
5	manipulation of critical information	severe	4
6	manipulation of information	minor	2
7	loss of critical information	significant	3
8	loss of critical information	significant	3
9	loss of critical information	significant	3
10	manipulation of critical information	severe	4
11	manipulation of critical information	severe	4
12	manipulation of critical information	severe	4
13	manipulation of critical information	severe	4
14	loss of critical information	significant	3
15	manipulation of critical information	severe	4
16	loss of critical information	significant	3
17	manipulation of critical information	severe	4
18	hazardous situation (steering)	catastrophic	5
19	loss of critical control	significant	3
20	loss of information	minor	2
21	hazardous situation (propulsion)	catastrophic	5
22	manipulation of information	minor	2
23	loss of critical information	significant	3
24	loss of critical information	significant	3

4.9 *Analysis of Risks*

The study identified a total of 24 risks associated with the INS. Of these, six were based on previous cyber incidents, 15 were identified through experimental methods, and six were based on realistic scenarios. Of the 24 risks, 14 were classified as low, eight as medium, and two as high. Two of the risks were specifically related to the GPS and the AIS and were deemed to be high. A graphical representation of the percentage of risks at each level is given in Figure 2.

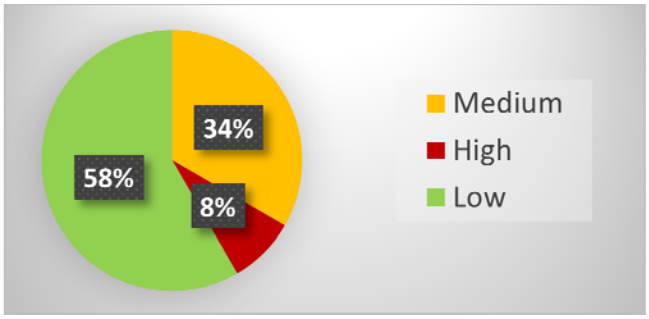

Figure 2. Risk levels

Table 11. Probability values

ID	Scenario	Research	Incident	Class	Score
1		[5]	[3]	likely	4
2		[5]		possible	3
3		[5]		possible	3
4		[5]		possible	3
5		[5]		possible	3
6		[5]		possible	3
7		[5]		possible	3
8		[5]		possible	3
9		[15]	[14]	likely	4
10		[6]	[13]	likely	4
11		[12]		possible	3
12		[12]		possible	3
13		[45]		possible	3
14			[34]	likely	4
15		[29]		possible	3
16			[7]	likely	4
17		[11]		possible	3
18			[8]	likely	4
19	✓			unlikely	2
20	✓			unlikely	2
21	✓			unlikely	2
22	✓			unlikely	2
23	✓			unlikely	2
24	✓			unlikely	2

5 VALIDATION

Method validation in this case consists of two phases, namely validating the results and validating the user-friendliness of the method. In order to validate the results, we compared our findings with the voluntary guidelines provided by [24]. These guidelines came to the fore in the IMO in 2022 [21]. In addition to iTrust, the Maritime and Port Authority of Singapore (MPA) contributed to the development of the guidelines [24]. The traditional risk assessment formula, *Risk = Severity×Likelihood*, was used in the study to assess risks at three levels: high, medium, and low. We compared the risk levels in [24] to those derived by CRASH and found that seven of them were the same, as shown in Table 14. Moreover, five of these risks were assessed at the same risk level.

In the second phase of the validation process we tested the user-friendliness of our method by means of interviews with 10 marine professionals, as shown in Table 15. The Table also depicts the reason for selecting each individual interviewee, so as to ensure a broad spectrum of expertise and experience.

We prepared a presentation in two parts. The first part described the method. The second part presented an example risk assessment for GPS jamming and GPS spoofing attacks. The presentation was sent to interviewees via e-mail before the interview. During the interviews a different example, not seen by the interviewees before the interview, was used. In the interviews, we first explained how CRASH works. Then, we discussed how the cyber risks of GPS jamming and GPS spoofing were assessed. Finally, the interviewees were invited to assess the risk of AIS ship spoofing by applying CRASH on their own.

Table 15. List of Interviewees in the Focus Group

#	Competency	Reason for selection
1	Oceangoing Watchkeeping Officer	Ship Cyber Security Officer; Giving training onboard to seafarers about the cyber risks of ships.
2	Oceangoing Chief Engineer	Maritime cyber security consultant; (Ex) Company Cyber Security Officer; Developing Cyber Security Plan, including risk assessment; Giving training onboard and at the office to seafarers about the cyber risks of ships.
3	Oceangoing Master	Completed M.Sc. thesis on maritime cyber security
4	Oceangoing Master	Developing a Cyber Security Plan, including risk assessment.
5	Oceangoing Chief Engineer	Experienced in safety risk assessments.
6	Oceangoing Master	Giving training at the office to seafarers about the cyber risks of ships.
7	Oceangoing Chief Officer	Developing Cyber Security Plan, including risk assessment.
8	Oceangoing Chief Officer	Ship Cyber Security Officer; Giving training onboard to seafarers about the cyber risks of ships.
9	(Ex) Oceangoing Watchkeeping Officer	Ongoing PhD thesis on maritime cyber security.
10	(Ex) Oceangoing Watchkeeping Officer	Ongoing PhD thesis on maritime cyber security.

Table 12. Criticality values

ID	Component	Redundancy	Number of DC	Class	Score
1	AIS	unavailable	1	high	3
2	AIS	unavailable	1	high	3
3	AIS	unavailable	1	high	3
4	AIS	unavailable	1	high	3
5	AIS	unavailable	1	high	3
6	AIS	unavailable	1	high	3
7	AIS	unavailable	1	high	3
8	AIS	unavailable	1	high	3
9	GPS	unavailable	5	high	3
10	GPS	unavailable	5	high	3
11	RADAR	partly	0	low	1
12	RADAR	partly	0	low	1
13	RADAR	partly	0	low	1
14	RADAR	unavailable	0	medium	2
15	ECDIS	available	0	low	1
16	ECDIS	available	0	low	1
17	ECDIS	available	0	low	1
18	unknown	available	hazardous situation	medium	2
19	RADAR	partly	0	low	1
20	AIS	unavailable	1	high	3
21	Controls for M/E	available	0	low	1
22	Indicator	available	0	low	1
23	BNWAS	unavailable	0	low	1
24	MFD	unavailable	0	low	1

DC: Dependent Component

The interviewees, except for those among them that are Ph.D. candidates, were not familiar with technical aspects of cybersecurity attacks such as GPS spoofing, GPS jamming, and AIS ship spoofing. However, they had experienced GPS jamming attacks during their sea services and were aware of hazardous situations, such as loss of steering, propulsion, and inert gas system. They were also not familiar with terms like loss of control, loss of

information, and manipulation of information; these had to be explained to them. Then, the interviewees were invited to answer the following questions:

- Does the AIS ship spoofing attack regard control or information? (correct answer: information);
- Does the AIS ship spoofing attack regard loss or manipulation of information? (correct answer: manipulation)
- Is the AIS ship spoofing attack critical or uncritical? (correct answer: critical).

The severity of the AIS ship spoofing attack was successfully, quickly, easily, and consistently by all interviewees identified as Manipulation of Critical Information.

During the interview, three risks related to AIS and GPS components were discussed. Although GPS jamming was known by all professionals, GPS spoofing and AIS ship spoofing attacks were not familiar to everyone. Consequently, determining the probability of spoofing attacks was challenging for some professionals. Therefore, it appears that the probability of known or recently experienced attacks in the industry can be more easily determined by professionals.

Redundancy and dependency components for the AIS and GPS were successfully identified by all interviewees. According to the interviewees, the design of the criticality matrix was confusing. As a result, this was re-designed by taking into account the suggestions of the interviewees, as shown in Table 4. During the interview, it was observed that a junior officer who had served for less than three months as OOW was not fully familiar with the bridge network. Therefore, he might have made an error in the dependency element if a risk related to a bridge component other than

Table 13. Risk numeric scores and qualitative levels

ID	Severity	Probability	Criticality	Risk score	Risk level
1	4	4	3	48	high
2	4	3	3	36	medium
3	4	3	3	36	medium
4	2	3	3	18	low
5	4	3	3	36	medium
6	2	3	3	18	low
7	3	3	3	27	medium
8	3	3	3	27	medium
9	3	4	3	36	medium
10	4	4	3	48	high
11	4	3	1	12	low
12	4	3	1	12	low
13	4	3	1	12	low
14	3	4	2	24	medium
15	4	3	1	12	low
16	3	4	1	12	low
17	4	3	1	12	low
18	5	4	2	40	medium
19	3	2	1	6	low
20	2	2	3	12	low
21	5	2	1	10	low
22	2	2	1	4	low
23	3	2	1	6	low
24	3	2	1	6	low

Table 14. Comparison of Risk Levels

ID	Comparison of Risk Levels		Results
	Our Study	Reference Study	
1	high	high	✓
7	medium	medium	✓
8	medium	medium	✓
9	medium	medium	✓
10	high	high	✓
12	low	high	x
16	low	high	x

GPS and AIS was given as an example. It was concluded that sea service might be necessary to determine the criticality element accurately.

6 CONCLUSION

Maritime transportation is a crucial component of global trade, and vessels are central to this mode of transport. However, with the increasing prevalence of computerized systems on modern vessels, including the Integrated Navigation System (INS), cyber threats have become a significant concern.

No statistics for maritime cyber incidents can be found in the literature. However, statistical data can be very useful in determining the probability of risks. Without such data, risk assessments can be subjective and depend too heavily on expert judgement. This paper proposed a CRASH, a method for assessing the safety impact of cyber risks onboard ships. CRASH is a combination of subjective and objective approaches: Probability and criticality are objective elements of risk, whereas the importance of control and information should be assessed as critical or non-critical by an expert, making the determination of severity somewhat subjective.

CRASH has significant advantages: its application is easy and does not require the use of software. Furthermore, the method reduces the need for expert judgements. Lastly, it is similar to the traditional maritime risk assessment formula, making it easy for experienced professionals with a maritime background to familiarize themselves with and apply. Indicative of this is the fact that even though interviewee #5 (in Table 15) was not fully aware of cyber risks, he successfully applied the method. Thus, CRASH can be used by ship operators to perform effective cyber risk assessments instead of relying on subjectively selected likelihood and severity values in traditional risk assessment methods.

However, CRASH also has some drawbacks: it requires a thorough assessment of cyber risks, including known vulnerabilities and past cyber incidents, which must be obtained from the literature and experience. Additionally, technical and operational details of the vessel are necessary, and sea experience is crucial to identifying dependencies and redundancies of compromised components. 24 risks associated with the INS were assessed in this paper. By applying CRASH, the study assessed 18 risks as low, 8 risks as medium, and 2 risks as high, highlighting the importance of having appropriate risk mitigation measures in place. Future studies could use CRASH to assess the cyber risks of systems

in other locations onboard, such as the engine room or the cargo control room.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to experts for their comments towards improving our study.
This paper has received funding from the Research Council of Norway through the Maritime Cyber Resilience (MarCy, project number 295077) project and the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS, project number 310105). The content reflects only the authors' views, and neither the Research Council of Norway nor the project partners are responsible for any use that may be made of the information it contains.

REFERENCES

[1] Emre Akyüz. "Application of fuzzy FMEA to perform an extensive risk analysis in maritime transportation engineering". In: International Journal Maritime Engineering 159.A1 (2017). DOI: 10.5750/ijme.v159iA1. 1013.

[2] Emre Akyüz and Erkan Çelik. "A quantitative risk analysis by using interval type-2 fuzzy FMEA approach: the case of oil spill". In: Maritime Policy & Management 45.8 (2018), pp. 979–994. ISSN: 0308-8839. DOI: 10.1080/03088839.2018.1520401.

[3] Andrej Androjna et al. "Assessing cyber challenges of maritime navigation". In: Journal of Marine Science and Engineering 8.10 (2020), p. 776. DOI: 10.3390/jmse8100776.

[4] H. Arabian-Hoseynabadi, H. Oraee, and P. J. Tavner. "Failure Modes and Effects Analysis (FMEA) for wind turbines". In: International Journal of Electrical Power & Energy Systems 32.7 (2010), pp. 817–824. ISSN: 01420615. DOI: 10.1016/j.ijepes.2010.01.019.

[5] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. "A security evaluation of AIS Automated Identification System". In: ACSAC'14: Proceedings of the 30th Annual Computer Security Applications Conference. Ed. by Charles N. Payne et al. New York, NY, USA: Association for Computing Machinery, 2014, pp. 436–445. DOI: 10.1145/2664243.2664257.

[6] Jahshan Bhatti and Todd E. Humphreys. "Hostile control of ships via false GPS signals: Demonstration and detection". In: Journal of the Institute of Navigation 64.1 (2017), pp. 51–66. DOI: 10.1002/navi.183.

[7] BIMCO et al. The guidelines on cyber security onboard ships. 2020. URL: https://www.ics-shipping.org/ wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (visited on 04/16/2023).

[8] Tanya Blake. Hackers took 'full control' of container ship's navigation systems for 10 hours - IHS Fairplay. 2017. URL: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships- navigation-systems-for-10-hours-ihs-fairplay/ (visited on 04/16/2023).

[9] Victor Bolbot et al. "A novel cyber-risk assessment method for ship systems". In: Safety Science 131 (2020). ISSN: 09257535. DOI: 10.1016/j.ssci.2020.104908.

[10] C4ADS. Above us only stars. 2019. URL: https : / / c4ads . org / wp - content / uploads / 2022 / 05 / AboveUsOnlyStars-Report.pdf (visited on 04/15/2023).

[11] Northern California Area Maritime Security Committee. Cyber security newsletter. 2014. URL: https://www. sfmx.org/wp-content/uploads/2017/03/Cyber- Security- Newsletter-2014- 1.pdf (visited on 04/16/2023).

[12] Maritime Executive. Tests show ease of hacking ECDIS, RADAR and machinery. 2017. URL: https://www. maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery (visited on 04/16/2023).

[13] Dana Goward. Mass GPS spoofing attack in Black Sea? 2017. URL: https://www.maritime-executive. com/editorials/mass-gps-spoofing-attack-in-black-sea (visited on 04/16/2023).

[14] Luke Graham. Shipping industry vulnerable to cyber attacks and GPS jamming. 2017. URL: https://www.cnbc. com/2017/02/01/shipping- industry- vulnerable- to-cyber- attacks- and- gps- jamming.html (visited on 04/16/2023).

[15] Alan Grant et al. "GPS jamming and the impact on maritime navigation". In: Journal of Navigation 62.2 (2009), pp. 173–187. DOI: 10.1017/S0373463308005213.

[16] Stanisław Gucma and Wojciech S´ la˛czka. "Comprehensive method of formal safety assessment of ship manoeu- vring in waterways". In: Scientific Journals of the Maritime University of Szczecin 54.126 (2018), pp. 110–119. URL: https://repository.am.szczecin.pl/handle/123456789/2473 (visited on 04/16/2023).

[17] Muhammet Gül and Erkan Çelik. "Fuzzy rule-based Fine-Kinney risk assessment approach for rail transportation systems". In: Human and Ecological Risk Assessment: An International Journal 24.7 (2018), pp. 1786–1812. ISSN: 1080-7039. DOI: 10.1080/10807039.2017.1422975.

[18] Todd E. Humphreys et al. "Assessing the spooing threat: Development of a portable GPS civilian spoofer". In: Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008). ION, 2008, pp. 2314–2325. URL: https://www.ion.org/publications/abstract. cfm?articleID=8132 (visited on 04/16/2023).

[19] IEC. IEC 63154 Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results. Geneva, Switzerland, 2021.

[20] IMO. International Safety Management (ISM) Code: Part A Chapter 10 Maintenance of the ship and equipment. London, UK, 2008.

[21] IMO. MSC 105/8/2 Measures to enhance maritime security. Voluntary cyber risk management guidelines for shipboard operational technology (OT) systems. London, UK, 2022.

[22] IMO. Resolution MSC.252(83) Adoption of the revised performance standards for Integrated Navigation Systems (INS), Introduction, Contents, Module A-B. London, UK, 2018.

[23] IMO. Resolution MSC.428(98) Maritime cyber risk management in Safety Management Systems. London, UK, 2017.

[24] iTrust. Guidelines for cyber risk management in shipboard operational technology systems. 2022. URL: https:// itrust. sutd. edu. sg/ news- events/ news/ guidelines- for- cyber- risk- management- in- shipboard-ot-systems/ (visited on 04/16/2023).

[25] Georgios Kavallieratos and Sokratis Katsikas. "Managing cyber security risks of the cyber-enabled ship". In: Journal of Marine Science and Engineering 8.10 (2020), p. 768. DOI: 10.3390/jmse8100768.

[26] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. "Cyber-attacks against the autonomous ship". In: Computer Security. Ed. by Sokratis K. Katsikas et al. Vol. 11387. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019, pp. 20–36. DOI: 10.1007/978-3-030-12786-2_2.

[27] Gary C Kessler, J Philip Craiger, and Jon C Haass. "A taxonomy framework for maritime cybersecurity: A demonstration using the Automatic Identification System". In: TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 12.3 (2018), p. 429. DOI: 10.12716/1001.12.03.01.

[28] G. Fine Kinney and A. D. Wiruth. Practical risk analysis for safety management. China Lake, California, USA, 1976. URL: https://apps.dtic.mil/sti/citations/ADA027189 (visited on 04/16/2023).
[29] Mass Soldal Lund, Odd Sveinung Hareide, and Øyvind Jøsok. "An attack on an Integrated Navigation System". In: Necesse 3.2 (2018), pp. 149–163. DOI: 10.21339/2464-353x.3.2.149.
[30] Mass Soldal Lund et al. "Integrity of Integrated Navigation Systems". In: 2018 IEEE Conference on Communica- tions and Network Security (CNS). IEEE, 2018. DOI: 10.1109/CNS.2018.8433151.
[31] B. Malekmohammadi and L. Rahimi Blouchi. "Ecological risk assessment of wetland ecosystems using Multi Criteria Decision Making and Geographic Information System". In: Ecological Indicators 41 (2014), pp. 133– 144. ISSN: 1470160X. DOI: 10.1016/j.ecolind.2014.01.038.
[32] Per Håkon Meland et al. "A retrospective analysis of maritime cyber security incidents". In: TransNav: Interna- tional Journal on Marine Navigation and Safety of Sea Transportation 15 (2021). DOI: 10.12716/1001.15. 03.04.
[33] Per Håkon Meland et al. "Assessing cyber threats for storyless systems". In: Journal of Information Security and Applications 64 (2022), p. 103050. ISSN: 22142126. DOI: 10.1016/j.jisa.2021.103050.
[34] Voltaire Network. What spooked the USS Donald Cook so much in the Black Sea? 2014. URL: https://www. voltairenet.org/article185860.html (visited on 04/16/2023).
[35] NIST. Guide for conducting risk assessments. Gaithersburg, MD, USA, 2012. DOI: 10.6028/NIST.SP.800- 30r1. URL: https : / / nvlpubs . nist . gov / nistpubs / Legacy / SP / nistspecialpublication800 - 30r1.pdf.
[36] OCIMF. Safety critical equipment and-spare parts guidance. 2018. URL: https : / / www . ocimf . org / document- libary/93- safety- critical- equipment- and-spare- parts- guidance/file (visited on 04/16/2023).
[37] Aybars Oruc. "Claims of state-sponsored cyberattack in the maritime industry". In: The International Naval Engineering Conference and Exhibition (INEC 2020). 2020.
[38] Aybars Oruc. "Cybersecurity risk assessment for tankers and defence methods". MSc. Istanbul, Turkey: Piri Reis University, 2020. URL: http://openaccess.pirireis.edu.tr/xmlui/handle/20.500.12960/52? locale-attribute=en (visited on 04/16/2023).
[39] Aybars Oruc, Ahmed Amro, and Vasileios Gkioulos. "Assessing cyber risks of an INS using the MITRE ATT&CK framework". In: Sensors 22.22 (2022). DOI: 10.3390/s22228745.
[40] Aybars Oruc, Vasileios Gkioulos, and Sokratis Katsikas. "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)". In: Journal of Marine Science and Engineering 10.1 (2022), p. 107. DOI: 10.3390/jmse10010107.
[41] Celia Paulsen and Patricia Toth. Small business information security: The fundamentals. Gaithersburg, MD, USA, 2016. DOI: 10.6028/NIST.IR.7621. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf (visited on 04/16/2023).
[42] Wenli Shang et al. "Information security risk assessment method for ship control system based on Fuzzy Sets and Attack Trees". In: Security and Communication Networks (2019). ISSN: 1939-0114. DOI: 10.1155/2019/ 3574675.
[43] Boris Svilicic et al. "A study on cyber security threats in a shipboard Integrated Navigational System". In: Journal of Marine Science and Engineering 7.10 (2019), p. 364. DOI: 10.3390/jmse7100364.
[44] Boris Svilicic et al. "Maritime cyber risk management: An experimental ship assessment". In: Journal of Navigation 72.5 (2019), pp. 1108–1120. DOI: 10.1017/S0373463318001157.
[45] Boris Svilicic et al. "Towards a cyber secure shipboard radar". In: Journal of Marine Science and Engineering 7.10 (2020). DOI: 10.1017/S0373463319000808.
[46] Kimberly Tam and Kevin Jones. "MaCRA: a model-based framework for maritime cyber-risk assessment". In:WMU Journal of Maritime Affairs 18.1 (2019), pp. 129–163. DOI: 10.1007/s13437-019-00162-2.
[47] UMT. Severity, Exposure & Probability (SEP) risk assessment model. URL: https : / / winapps . umt . edu/ winapps/ media2 / wilderness/ toolboxes/ documents/ safety/ Severity, %20Exposure% 20 &%20Probability%20(SEP)%20Risk%20Assessment%20 Model.pdf (visited on 04/16/2023).
[48] UNCTAD. Review of maritime transport 2021. New York, USA, 2021. URL: https://unctad.org/webflyer/review-maritime-transport-2021 (visited on 04/16/2023).