Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P143-cd

Safety and security integrated analysis approaches considering new updates for maritime systems

Rogério Brito Ramos

Safety Analysis Group, Computer Engineering and Digital Systems Department, University of São Paulo, Brazil.
E-mail: rogerio.ramos@usp.br

João Batista Camargo Júnior

Safety Analysis Group, Computer Engineering and Digital Systems Department, University of São Paulo, Brazil.
E-mail: joaocamargo@usp.br

As the modern ships have their operation dependent on information systems, a cyber-attack can impact the safety objectives. Cyber security analysis (related to protection against malicious attack) has become part of the modern design system as well as traditional safety analysis (related to prevention from accidents). However, both disciplines are usually performed in distinct or weak linked processes, which to succeed rely on exhaustive tasks and on the expertise of the analysts. Combined analysis approaches are required to provide a straightforward identification of safety and security issues, once it is possible that a countermeasure to minimize a safety issue can expose a security vulnerability, and a deployment to fix a security question could also bring new safety hazards. The purpose of this paper is to present the characteristics of some selected safety and security integrated analysis approaches applied to a case study with technologies deployed in maritime systems. The results suggested that the approaches can be useful to capture vulnerabilities, hazards and conflicts that could not be detected by a separated or empirical analysis. Another conclusion is that to select a suitable approach should be part of a safety and security analysis process. For future works, those steps can be extended to other types of critical systems.

Keywords: safety and security integrated, ship systems, maritime systems, Cyber Physical System (CPS), vulnerabilities, hazards and cybersecurity.

1. Introduction

Due to strategic business matters the ship control and supervision systems have their architecture constantly updated, incorporating new technologies such as Internet of Things (IOT), wireless communication, sensor and actuator with new hardware, cloud and fog computing and even machine learning features are considered as alternatives. These new deployments imply that these systems can be categorized as a Cyber Physical System (CPS) where a cyber-attack may directly reach a physical consequence.

In this study, security is related to the capacity to protect a system from a malicious intervention, while safety is related to the prevention from accidents. Safety analysis is traditionally mandatory in the design ships and there are many known techniques such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) that guide the engineers to identify critical components and apply changes to increase the safety levels. Besides that, as the information systems are present in the ships operation, cybersecurity analysis should always be taken into consideration. However, it is still strongly recommended that safety and security analysis be performed in a joint manner, and one good reason for this is the possibility that a countermeasure applied to increase the safety level may expose a security vulnerability, and vice versa, a patch applied to fix a security question may have a negative safety impact. Therefore, a modification on one side needs to be evaluated on the other.

The current approaches to capture safety and security issues should be frequently assessed and updated whenever a new resource is adopted in the development system. Although at the same time a new feature brings functionalities

advantages, it also may carry new security vulnerabilities and safety hazards that may not be covered by the approaches.

The purpose of this paper is to present an overview of some selected safety and security integrated analysis approaches, to apply them to a case study and present the results of scenarios with or without security countermeasures implemented. In this paper, in section 2, we mention some selected methods to perform safety and integrated analysis. In section 3 we highlight some new characteristics of maritime systems. In section 4, we present a case study. And finally, in section 5, our conclusion and perspective to future works are exposed.

2. Related works

Since Information Systems have become part of critical applications, the cybersecurity discipline started to be incorporated into safety analysis. Kriaa et al. (2019) argued that combined approaches could be classified as process-oriented which are more related to the high level of the system, based on the general safety and security requirements. However, they may not be enough to catch technical issues from the lowest levels of the system. The other group, named model-based, is closely related to math models such as Markov Chains, and is more appropriate to get quantitative results, however it requires further effort to adapt new technologies and estimate parameters.

Di Maio et al. (2020) also mentioned the Goal Tree Success Tree Master Logic Diagram (GTST-MDL) method and define it as a goal-oriented approach that is able to consider failures and cybersecurity threats and providing quantitative results. In this work we highlight two methods that enables formal modelling based on mathematical concepts, Markov Chains, and allow qualitative and quantitative results. And we also highlight a process-based method that is suitable to apply in the early phases of the design.

2.1. *The S-cube approach*

Kriaa et al. (2019) proposed the S-cube model-based approach for SCADA (supervisory control and data acquisition) systems that provides possible risk scenarios with safety and security aspects to industrial information and control architecture. The S-cube has as input the system architecture and as output the attack and failure scenarios that may result in an undesirable condition. In the S-Cube, there is the S-cube KB component which is a specific language based on Figaro (Khan et al., 2021) that allows to describe the digital assets with safety and security properties. The results generated by the S-cube KB component go to quantification tools such as YAMS, a Monte Carlo simulator, and Figseq, a tool for systems reliability and availability calculator. Finally, the attack and failure scenarios are generated to guide the safety analysts to make decisions about the system. These steps are depicted in figure 1.

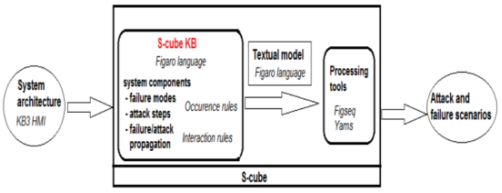

Fig. 1. The S-Cube diagram (Kriaa et al. 2019).

The system architecture should be translated to a knowledge base in figaro language compatible with S-cube KB. Whenever a new system modification is applied, all the S-cube processes should be performed again. This approach gives a good opportunity to expand to other types of systems by adapting the S-cube KB component. Oueidat et al. (2022) presented an approach based on the same principle, using knowledge base, and generated automatically attack scenarios and linking them with safety risks.

2.2. *The CHASSI method*

Raspotnig et al. (2012) proposed the CHASSI (Combined Harm Assessment of Safety and Security for Information systems) method that is based on UML (Unified Modelling Language) notations and it aims to assess safety and security aspects. Basically, this method is divided into three main stages: Eliciting Functional Requirements, Eliciting Safety/Security Requirements and Specifying Safety/Security Requirements. All the stages and activities are shown in figure 2. In the first stage named Eliciting Functional Requirements are defined the global functions and services and elaborated the UML Use Case and the Sequence Diagrams. In the second stage, Eliciting Safety/Security Requirements, Misuse Case Diagrams based on HAZOP technique and Misuse/Failure Sequence

Diagrams are created. The aim is to identify vulnerabilities and try to mitigate them, both safety and security are seen and may be treated together. The last stage, Specifying Safety/Security Requirements, after receiving the inputs from a HAZOP table, the Safety and Security requirements are ready.

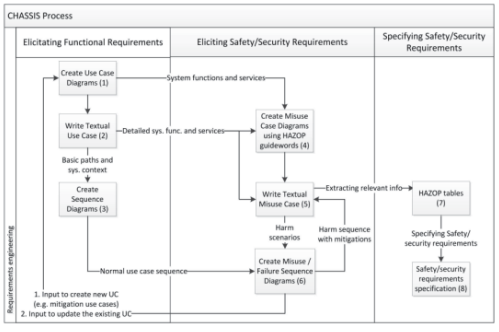

Fig. 2. The CHASSIS Process (Raspotnig et al., 2012)

The CHASSIS method only provides qualitative results. If a quantitative is required it will need to match with other tools. In another study Raspotnig et al. (2018) described that the CHASSI method was successfully to capture safety and security issues when assessing small to medium sized suppliers to the air-traffic management (ATM) sector.

2.3. The *BDPM formalism*

The BDMP (Boolean logic Driven Markov Processes) was proposed by Bouissou (2008) initially for only safety analysis as an alternative to Fault Tree but later adapted by Pietre-Cambacedes and Bouissou (2010) to include security aspects. Recently, Czekster and Morisset (2021) presented the tool BDMPathfinder that aims to explore possible attacks considering the progression over time.

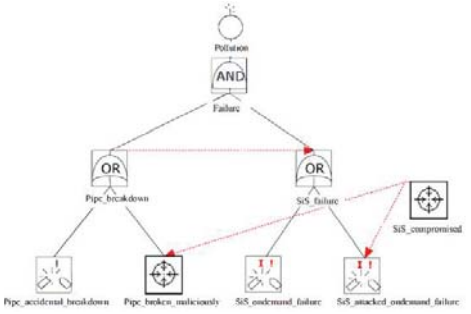

Fig. 3. A BDMP model with safety and security events (Czekster and Morisset, 2021)

The dotted arrows shown in figure 3 are triggers, that are responsible to differ BDMP from traditional fault trees providing a dynamic behaviour matching BDMP with Markov models. A trigger basically means that the arrow target event is considered only if the previous happens.

The BDMP are compounds of Knowledge Bases written in Figaro Language that can be carried in the proprietary software called RiskSpectrum ModelBuilder, and then building the graphical tree structure, setting parameters and simulating. With RiskSPectrum it is also possible to export the results and import them to the YAMS tool (Another Monte Carlo Simulator). This formalism allows us to model any kind of system.

3. The maritime systems characteristics

The current ships designed nowadays are full of information system technologies and old ships tend to have their system gradually updated with cutting-edge assets. This tendency is connected to business matters that also comprises safety objectives. These new kinds of implementation allow a ship to be accessed and monitored remotely, allowing the captain to visualize the data from all internal sensors. All these advantages provided by those updates also bring complex challenges to the safety analysts to identify the new types of risk associated. These systems now can be denominated as Cyber Physical System (CPS) where a cyber vulnerability can be explored.

A Safety and Security Integrated Analysis is strongly recommended to avoid any undesirable result. It is justifiable this argument if we assume for instance, the need to deploy a wireless communication between a controller and an actuator. If this communication were implemented with authentication and encryption processes, we can assume that the security level increases, but the safety level decreases, once these processes introduce latency. On the other hand, if we let this communication in clear mode, reducing latency and increasing safety level, it will easily be susceptible to interception, decreasing security level. Therefore, a suitable approach is required to capture this type of antagonism and guide engineers to make a decision. Additionally, Shipunov et al. (2021) listed some cyber-attacks suffered by Maersk in 2017, China Ocean Shipping Company (COSCO) in 2018, and US Coast Guard in 2019.

A complete maritime information system can be a compound of on-board systems, off-shore systems and communication networks. Ashraf et al. (2023) mentioned this classification and listed some classes of systems:

- Automatic Identification System (AIS) is responsible to provide safe navigation, avoiding collision with other ships by communication with them. The AIS is vulnerable to false reproduction where a ghost ship can be created to disturb the course of other ships. An oil ship used falsified AIS data and pretended to be Tanzanian to navigate to Syria according to The Maritime Executive (2023). Balduzzi et al. (2014) have conducted a detailed security evaluation of AIS.
- Electronic Chart Display and Information System (ECDIS) corresponds to the interface that shows to the crew the data of the ship and its route. It is connected to an external network to collect data from off-shore systems, and also is connected to the sensor of the ship. The data shown need to be available and be trusty.
- Global Navigation Satellite System (GNSS) is responsible for providing data from GPS to navigation. They are vulnerable to jamming and spoofing attacks. Androjna and Perkovič (2021) detailed how these attacks could impact navigation.
- Navigation Telex (NAVTEX) is responsible for providing meteorological information and other urgent data from the Port Authorities to the ships. This system is connected to the internet and consequently vulnerable to diverse attacks.
- Voyage Data Recorders (VDR) is similar to a black box flight recorder, the VDR is responsible for storing the voyage details of the ship. As the VDR is connected to all components of the ship, if an attacker with access to the local network reaches the VDR, he also can reach many digital components.
- GMDSS (Global Maritime Distress and Safety System): is responsible for request search and rescue support. Distress messages are sent to other ships and to shores. It is vulnerable to spoof and jamming attacks, therefore, these attacks can disturb ships and shores and put in extreme risk a real rescue operation.
- SCADA (Supervisory control and data acquisition): responsible for monitoring and displaying status and alarms for internal assets such as: propulsion, engines, generators, tanks, pumps and many other sensors. It usually involves IoT components with limited resources and communications are done in wireless protocol. Some SCADA deployments converge in Cloud and Fog architecture as can be seen in Qiu et al. (2018).

4. A case study: anti-heeling system

The anti-heeling system is responsible to detect the heeling angle and adjust it in order to avoid that the ship topples and sinks. This system basically is a compound of: sensors that detect angle, ballast tanks that are compartments which can be filled with water and air in order to provide stability to the ship, actuators that operates ballast tanks, a unit processor that receives data from sensors and sends them to the actuators, valves that control the flow of ballast tanks, pipes, pressure valves and pump. Figure 4 shows an example of the Anti-Heeling System with one ballast tank on each side of the ship.

In this study we will check the safety attribute by building manually the Fault Tree and Markov Chains diagrams which are the core of S-CUBE and BDMP. The steps performed here can done automatically by those approaches, so the results should be same. The CHASSIS method is not covered but it can be useful to build the fault tree used in this case study.

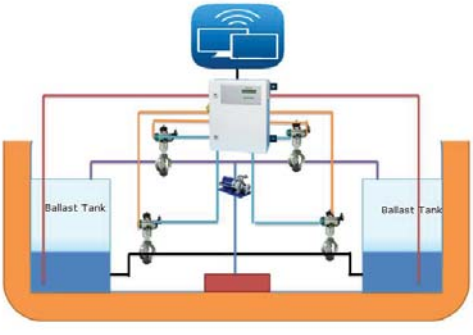

Fig. 4. An example of Anti-Heeling arrangement with ballast tanks shown (Atlas Marine, 2023)

In this case study we abstract the components and will consider the only following modules:

- The angle sensors: identify the ship angle and send it to the unit processor in an interval of 100ms.
- The board computer: receive data from the sensor, check if the values are acceptable. Case negative, identify the ballast tank that needs to be operated and send the instruction.
- The ballast tanks actuators: receive command from the unit processor to fill with water or air or to stop. We consider two ballast tanks: one located at port (left side) and the other at starboard (right side).
- The SHIP: needs to be balanced, the heeling angle cannot be over the limits. Otherwise, a ship will tend to topple.

The purpose of this case study is to compare the safety impact of two scenarios: one with encrypted communication and authentication method deployed, and the other with clear mode and without authentication.

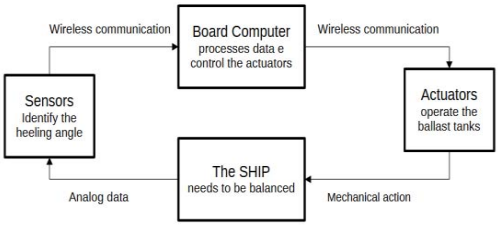

Fig. 5. Anti-Heeling diagram

The figure 5 depicts the modules of our Anti-Heeling system and the communication among sensors, board computer and actuators are wireless, and susceptible to malicious intervention.

The figure 6 represents the Fault Tree of the Anti-Heeling System considering two types of cyber-attacks, jamming and spoofing. In this tree we notice that it is possible to reach the Top Event "SHIP TOPPLED" from a "SPOOFING ATTACK" succeeded and a malicious operation in the ballast tanks represented by "TANKS OPER". The leaf "JAMMING ATTACK" impacts the unavailability of the Anti-Heeling System, "AH UNAVAILABLE". However, it does not reach the top event yet unless the event "CARGO VARIATION" happens. We imply to this scenario that a spoofing attack can be more dangerous than a jamming attack.

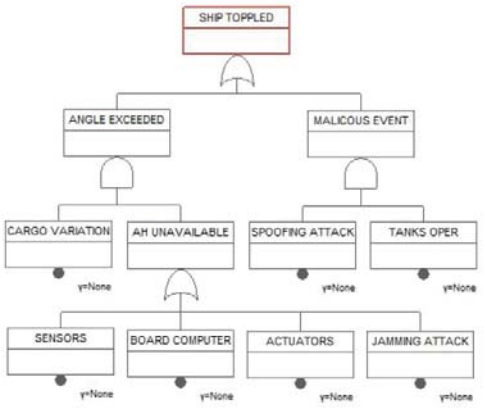

Fig. 6. Fault tree of the Anti-Heeling System

Next step, we will look into quantitative analysis representing the case study in Markov Chains. We started with a block diagram shown in figure 7 to guide us to mount the states and equations. In this diagram we assume that if the block M1 fails, that would represent a complete spoofing attack, the safety requirement is not attended. With M1 working, the safety requirement is not attended only if M4 and M2, or M4 and M3 fail. The safety requirement is still valid since the Eq. (1) results true:

$$Opr = M1\ (M2M3 + M4) = M1M2M3 + M1M4 \quad (1)$$

Now it can be represented by 3 states: P1 (which means the modules M1, M2 and M3 working), P2 (which means the modules M1 and M4 working) and PF (which means Failure "SHIP TOPPLED"). Only the P1 and P2 states indicate that the safety requirement is attended due to combination of modules that are still working.

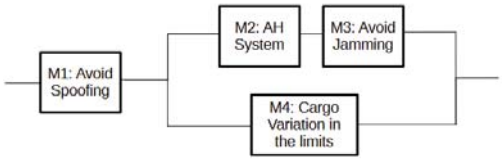

Fig. 7. Block Diagram to represent the relationship among the critical modules

The attribute coverture and repair will not be considered, we associate the:

- $\lambda 1$ to the probability of M1 fails, which means a successful and complete spoofing attack.

- λ2 to the M2 fails, which means that the sensor, computer board or actuator are not working, compromising the Anti-Healing System.
- λ3 to M3 fails, which means a successful jamming attack.
- λ4 to M4 fails: which means the probability to occur a cargo variation above the limits tolerated.

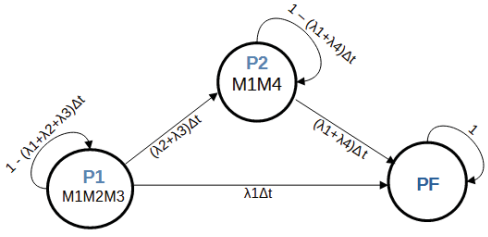

Fig. 8. Representation in Markov chains

The figure 8 represents the Anti-Heeling system in Markov Chains, and Δt represents the time variation. The next step is to elaborate the probability equation to be in each state:

$$P1(t + \Delta t) = (1-(\lambda1+\lambda2+\lambda3)\Delta t)\ P1(t) \quad (2)$$

$$P2(t + \Delta t)=(\lambda2+\lambda3)\Delta t P1(t)+ (1-(\lambda1+\lambda4)\Delta t)P2(t) \quad (3)$$

$$PF(t + \Delta t) = \lambda1\Delta t P1(t) + (\lambda1+\lambda4)\Delta t P2(t) +PF(t) \quad (4)$$

Now we transform the Eq. (2), Eq. (3) and Eq. (4), and differential equations Eq. (5), Eq. (6) e Eq. (7) respectively.

$$dP1(t) /dt = (\lambda1+\lambda2+\lambda3)P1(t) \quad (5)$$

$$dP2(t) /dt = (\lambda2+\lambda3)P1(t)+(\lambda1+\lambda4)P2(t) \quad (6)$$

$$dPF(t) /dt = \lambda1P1(t) + (\lambda1+\lambda4)P2(t) \quad (7)$$

We create a script in the MATLAB where the differentials equations are used as input, the values of λ1, λ2, λ3 and λ4 can be adjusted according to the estimation of the analyst. The script steps are described in Table 1. The failure rates are changed in each simulation.

Table 1. MATLAB script steps to output the safety function.

Step	Description
1	Set the failure rates: λ1=0.001, λ2 = 0.0005, λ3= 0.001 and λ4= 0.005;
2	Declare the probabilities functions as symbolic type: syms P1(t) P2(t) PF(t);
3	Set the differentials equations: edP1 = diff(P1,t) = = -(λ1+λ2+λ3)*P1; edP2 = diff(P2,t) = = (λ2+ λ3)*P1-(λ1+λ4)*P2; edPF = diff(PF,t) = = λ1*P1+(λ1+l λ4)*P2;
4	Declare the differential equations vectors: edos = [edP1; edP2; edPF];
5	Set the initial conditions: cond = [P1(0) = =1; P2(0) = =0; Pf(0) = =0];
6	Solve the differential equations: [P1sol(t), P2sol(t), PFsol(t)] = dsolve (edos,cond);
7	Sum the states that means the system is working: Safe=P1sol+P2sol;
8	Plot the function Safe (t)

Note the λ character is not accepted in MATLAB code, then it should be replaced by other characters.

To match with the proposal of this study we take into considerations the following kind of scenarios for the Anti-Heeling system:

- With security countermeasures: for instance, cryptography and authentication methods applied to communication among the modules. The λ1 and λ3 tend to drastically reduce while λ2 tends to increase due to latency introduced, the λ4 is not influenced.
- Without security countermeasures: all communications in clear mode, the λ1 and λ3 tend to drastically increase while λ2 tends to decrease, the λ4 is not influenced.

It is another challenge to estimate failure probability for the modules and attack probabilities. The lack of data from the past of a system and the new unknown safety characteristics can make those estimations poorly. However, as mentioned before, we can affirm that λ1 and λ3 are inversely proportional to λ2.

For the simulation A, figure 9, we set the following values: λ1=0.0001, λ2=0.0005, λ3=0.0001 and λ4 ==0.0005, and the reliability value at time 1000, Safe (1000) = 0.5635.

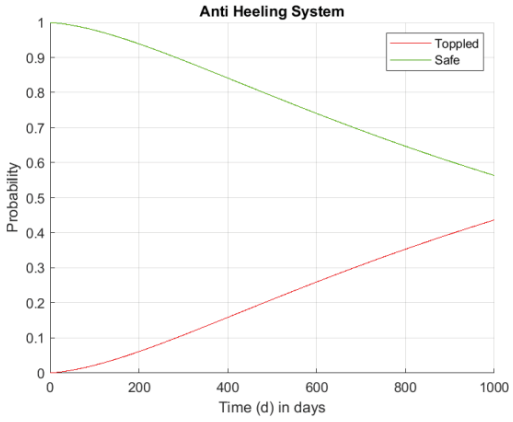

Fig. 9. Simulation A: without cryptography and authentication, LOW probability of cyber attacks

The simulation B, figure 10, we set the following values: λ1=0.000001, λ2=0.001, λ3=0.000001 and λ4 ==0.0005, and the reliability value at time 1000, Safe (1000) = 0.4574, worse than simulation A. In this scenario the security measures increased the chances of the ship toppling.

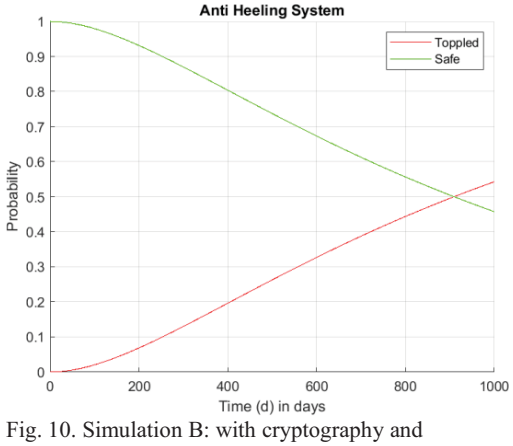

Fig. 10. Simulation B: with cryptography and authentication, too LOW probability of cyber attacks

For the simulation C, figure 11, we set the following values: λ1=0.001, λ2=0.0005, λ3=0.001 and λ4 =0.0005, and the reliability value at time 1000, Safe (1000) = 0.1162. In this scenario, we assumed a high probability of cyber-attacks and the security measures would drastically reduce the chances of the ship toppling.

From the results achieved with the simulations, we infer that not always a security measure can contribute to meet a safety requirement.

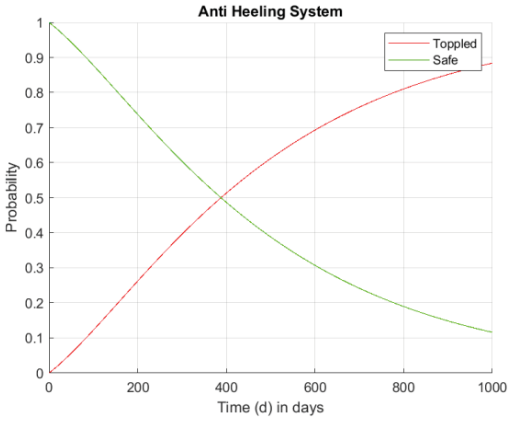

Fig. 11. Simulation C: without cryptography and authentication, HIGH probability of cyber attacks

From the perspective of the BDMP method, the Fault Tree shown in figure 6 would be the input and the outputs would be the functions shown in the figures 9, 10 e 11. From the S-Cube perspective, the input would be a description in Figaro language of the system architecture shown in figure 5 and the output would be the Fault Tree and the graphics shown in the figures 9, 10 e 11. And finally, from the CHASSIS perspective, the input would be a UML case diagram and the outputs the safety requirements.

5. Conclusion and future work

Through the development of this paper, it was noticed the importance of performing integrated analysis with safety and security aspects. This paper presented that the safety and security integrated analysis approaches, BDMP, S-cube and CHASSIS can be useful to manage vulnerabilities and hazards that could not be detected by an empirical analysis or separated methods. We mention the main systems deployed in the maritime industry, the vulnerabilities associated and the challenges with new technologies. Finally, we present a case study that consists of an Anti-Heeling automatic system and we perform a qualitative and quantitative analysis, the results suggest that we should care with securities implementation due to effects on safety levels. The novelty of this case study was to demonstrate that there are sets of fail and attack probability values where safety and security measures can be antagonists. As a perspective for future works, as from now on the information systems will be increasingly intertwined with safety conditions. New technologies such as cloud

and fog architecture, new IOT components, machine learning techniques need to have their characteristics mapped to the safety aspects.

Acknowledgement
The authors are grateful for the financial support from the Brazilian Navy. We appreciate RiskSpectrum AB Company for providing us an academic version of Risk Spectrum Model Builder and for helping us to master the software. We also thank the members of the Safety Analysis Group at the University of São Paulo for technical support on numerous issues during this research.

References

Androjna, A., and Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, *10*(2), 361–373.

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. Bin, and Nosheen, S. (2023). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690.

Atlas Marine. (2023). *AMS alarm system, Solution for Anti Heeling system*. http://atlasmarine.sg/alarm-system/, Accessed: 2023-03-23.

Balduzzi, M., Pasta, A., and Wilhoit, K. (2014). A security evaluation of AIS automated identification system. *ACM International Conference Proceeding Series*, *2014, 1*(1), 436–445.

Bouissou, M. (2008). BDMP (Boolean logic Driven Markov Processes) ® as an alternative to Event Trees Benchmark on dependability of complex dynamic systems. *Proceedings of the 17nd European Safety and Reliability Conference (ESREL 2008)*, 1779–1786.

Czekster, R. M., and Morisset, C. (2021). BDMPathfinder: a tool for exploring attack paths in models defined by Boolean logic Driven Markov Processes. *2021 17th European Dependable Computing Conference (EDCC)*, 83–86.

Di Maio, F., Mascherona, R., and Zio, E. (2020). Risk Analysis of Cyber-Physical Systems by GTST-MLD. *IEEE Systems Journal*, *14*(1), 1333–1340.

Khan, S., Volk, M., Katoen, J. P., Braibant, A., and Bouissou, M. (2021). Model Checking the Multi-Formalism Language FIGARO. *Proceedings - 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2021*, 463–470.

Kriaa, S., Bouissou, M., and Laarouchi, Y. (2019). A new safety and security risk analysis framework for industrial control systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *233*(2), 151–174.

Oueidat, T., Leva, M. C., Patelli, E., Podofillini, L., Wilson, S., Flaus, J.-M., and Massé, F. (2022). *A new way to generate automatically the attacks scenarios and combine them with safety risks*. 327–334. https://doi.org/10.3850/978-981-18-5183-4_R09-04-328-cd

Pietre-Cambacedes, L., and Bouissou, M. (2010). Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, 2852–2861.

Qiu, B., Zhang, Y., Wei, M., Li, Y., and Wang, Y. (2018, August 27). Hybrid Cloud Based Cyber-enabled Ship Control and Management System. *2018 IEEE International Conference on Prognostics and Health Management, ICPHM 2018*.

Raspotnig, C., Karpati, P., and Opdahl, A. L. (2018). Combined assessment of software safety and security requirements: An industrial evaluation of the CHASSIS method. *Journal of Cases on Information Technology*, *20*(1), 46–69.

Raspotnig, C., Peter Karpati, and Vikash Katta. (2012). A Combined Process for Elicitation and Analysis of Safety and Security Requirements. *EMMSAD 2012: Enterprise, Business-Process and Information Systems Modeling*, *1*, 347–361.

Shipunov, I. S., Nyrkov, A. P., Ryabenkov, M. U., Morozova, E. V., and Goloskokov, K. P. (2021). Investigation of Computer Incidents as an Important Component in the Security of Maritime Transportation. *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, 657–660.

The Maritime Executive. (2023). *Iran, Tanzania and Falsifying AIS Signals to Trade with Syria*. https://maritime-executive.com/article/iran-tanzania-and-falsifying-ais-signals-to-trade-with-syria. Accessed: 2023-03-23.