Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel

Carreras Guzman, Nelson Humberto; Kwame Minde Kufoalor, D.; Kozin, Igor; Lundteigen, Mary Ann

Published in:
Proceedings of the 29th European Safety and Reliability Conference

Publication date:
2019

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

Combined safety and security risk analysis using the UFoI-E method: A case study of an autonomous surface vessel

Nelson H. Carreras Guzman

Engineering Systems Group, Department of Technology, Management and Economics, Technical University of Denmark (DTU), Denmark. E-mail: nelca@dtu.dk

D. Kwame Minde Kufoalor

Center for Autonomous Marine Operations and Systems (AMOS), Department of Engineering Cybernetics, Norwegian University of Science and Technology (NTNU), Norway. E-mail: kwame.kufoalor@ntnu.no

Igor Kozine

Engineering Systems Group, Department of Technology, Management and Economics, Technical University of Denmark (DTU), Denmark. E-mail: igko@dtu.dk

Mary Ann Lundteigen

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology (NTNU), Norway. E-mail: mary.a.lundteigen@ntnu.no

Many standards consider safety and security risk analysis as separate fields, specifying the system specific safety or security issues and methods to analyze them. Having these separated fields of safety and security standards complicates the risk analysis of cyber-physical systems (CPSs), where safety and security issues coexist within the integrated layers of the system. Even though several integrated safety and security analysis methods exist in the literature, they are not tailored to assess the complex and tight interactions among the CPS layers and the system's surrounding environments. Therefore, this paper describes a method to conduct a combined safety and security risk analysis in CPSs for safety verification. Namely, we propose the Uncontrolled Flows of Information and Energy (UFoI-E) method, introducing novel diagrammatic representations to consider the dependencies within a CPS and its surrounding environments. As a case study, this paper describes a risk analysis of the collision avoidance function of an autonomous surface vessel, proving the convenience of examining the safety of autonomous vessels as safe and secure CPSs. The results of this paper may be input to new revisions and initiatives on new standards combining safety and security analysis.

Keywords: Safety and security, risk analysis, cyber-physical systems (CPSs), autonomous surface vessel, UFoI-E.

1. Introduction

The rising trend in control automation and information technologies supports the development of cyber-physical systems (CPSs), promising higher levels of performance, efficiency, and reliability in a wide set of applications (Rajkumar et al. 2010). We define CPSs as engineered systems that integrate information technologies, real-time control subsystems, physical components, and human operators to influence physical processes by means of cooperative and (semi)automated control functions. Some relevant applications include autonomous transportation, smart grids, and smart medical devices, among others.

However, new system interactions and complexities in CPSs also bring new challenges to ensure system safety. The integration of information technologies in networked systems and the higher automation levels complicate the risk analysis process to support safe design and operations. In these complex systems, loss events with safety implications – i.e. with the potential to induce physical harm to people, assets, or the natural environment – are not restricted to individual component failures. Instead, the complex interactions and feedback loops in these systems require a comprehensive analysis of the system architecture. In fact, small deviations in overlooked functional interactions among components could trigger unexpected and catastrophic consequences (Leveson 2011).

Moreover, security threats – i.e. deliberate sources of risk – are increasingly important factors leading to physical harm in CPSs. As evidenced by the Stuxnet attack to an Iranian nuclear facility in 2010 (Langner 2011), cybersecurity threats can propagate throughout the system, reach the control of physical processes and cause harm (Yampolskiy et al. 2013). Indeed, recent loss events and experimental research in smart vehicles, industrial control systems, smart grids and medical devices (Humayed et al. 2017) evidence

the appearance of new security scenarios that escape the traditional scope of safety risk analysis. Physical attacks (e.g. sabotage, theft) are also possible in targeted critical points if physical protection is lacking. These challenges require a safety and security integration in risk analysis (Aven 2007), (Pietre-Cambacedes and Bouissou 2013).

Having separated fields of safety and security standards complicates the risk analysis of CPSs, where safety and security issues coexist within the integrated layers of the system (Sun et al. 2009). On the one hand, safety standards provide guidance for safety requirements and analysis. These standards focus on accidental and environmental hazards as unintentional sources of physical risks to humans, assets, or the natural environment. On the other hand, security standards address security-related requirements and analysis in terms of confidentiality, integrity and availability goals in cyber systems. These standards focus mainly on deliberate threats and system vulnerabilities that pose risks to the security goals.

A need for integration of security to ensure safety is reflected in efforts for new standards and guidelines. IEC 62443 (IEC 2009) was published to provide security levels to industrial networked control systems (IACS), complementing the verification of safety-related systems and their safety integrity levels as defined in IEC 61508 (IEC 2010). Similarly, ISO/TR 22100-4 (ISO 2018) was recently published to provide guidance for cybersecurity in machinery, complementing safety guidelines in ISO 12100 (ISO 2011) for machinery. Moreover, several methods in the literature are aiming at integrating safety and security in CPSs (Chockalingam et al. 2013), (Kriaa et al. 2015), (Bolbot et al. 2018). Still, no current method sufficiently achieves a comprehensive analysis of the interactions among the CPS layers and system surrounding environments, preventing physical harm from a combined safety and security risk analysis (Zio 2018).

In this paper, we demonstrate the process to conduct a combined safety and security risk analysis of CPSs, illustrating the case of an autonomous surface vessel (ASV). First, we describe the Uncontrolled Flow of Information and Energy (UFoI-E) method, illustrating the CPS master diagram and the UFoI-E concept as convenient diagrammatic representations for risk analysis of CPSs. Second, we conduct the risk analysis for the collision avoidance system (CAS) of the ASV, i.e. the autonomous system responsible for avoiding collisions with surrounding obstacles while navigating at sea in autonomous mode. The aim of this analysis is to support the design and implementation of the CAS to prevent scenarios where anomalous situations due to unintentional incidents and deliberate attacks lead to unsafe behavior of the ASV.

2. UFoI-E method for combined safety and security risk analysis in CPSs

The Uncontrolled Flows of information and Energy (UFoI-E) method facilitates the integration of the safety and security standards in their current form. In addition, this method conceptualizes CPSs beyond the traditional scope of the safety and security standards, highlighting the need to consider higher-level system dependencies to understand and assess properly the resulting security implications for safety. In this section, we describe the CPS master diagram and the UFoI-E concept as the theoretical basis of the UFoI-E method for risk analysis.

2.1 *CPS master diagram*

Risk analysts acknowledge that we are not able to analyze a system as such, but only a conceptual model of the system (Rausand 2011). This limitation entails the challenge to represent the system in a way that is *comprehensible* to the analysts and *comprehensive* to incorporate all the relevant features needed for the analysis. In the context of CPSs, a valid representation must evidence the system components, interconnections and feedback control loops that characterize the system and its interaction with the environment. In this sense, the CPS master diagram represents a CPS as system layers and environments with interacting energy and information flows (Carreras Guzman et al., n.d.). As shown in *Fig. 1*, this representation conceives a CPS as the integration of cyber, cyber-physical and physical layers tightly coupled in feedback loops and interconnected with cyber and physical environments. This representation is an integration and a refinement of an abstract model for CPSs security (Humayed et al. 2017) and a systems-theoretic approach for system safety (Leveson 2011). The boundaries between the CPS and its environments are established according to the domain of control of the stakeholders under consideration. In other words, the functional performance of the processes within the CPS are under the responsibility of the stakeholder conducting the analysis (e.g. system designer, managers, and operators). The environmental influences, in turn, affect the system performance from processes beyond the control of the system stakeholder (e.g. natural conditions, external infrastructure services).

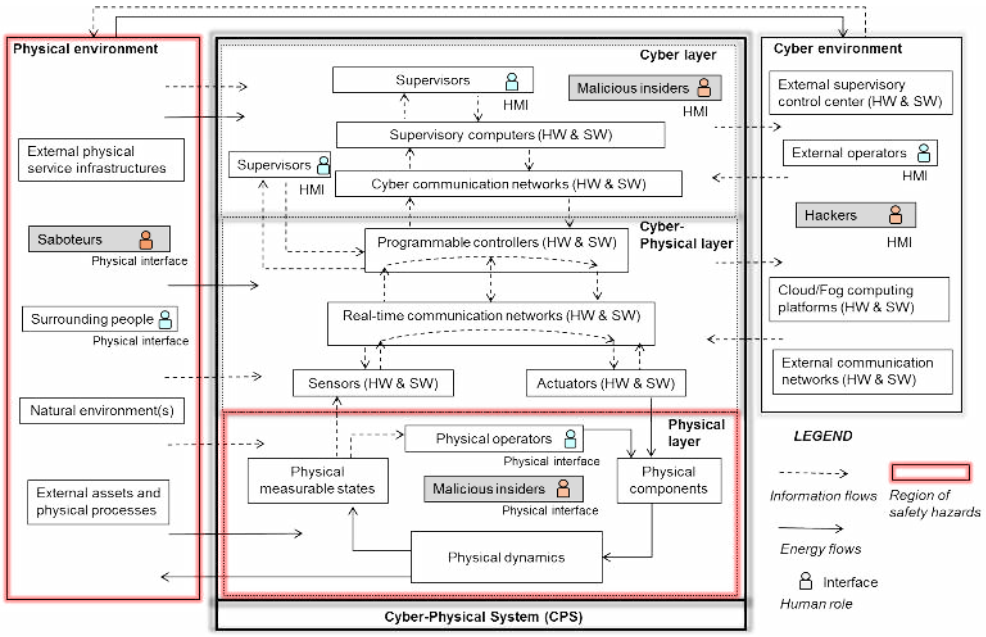

Fig. 1. Generic CPS master diagram

The CPS master diagram locates explicitly the region of safety hazards in the domain of energy, where the energy flows between the physical layer of the system and the physical environment could deviate into hazardous states. This feature makes the representation suitable for safety risk identification. Moreover, the sources of risk are not restricted to this domain, since information flows at the cyber-physical layer could influence the physical layer in unsafe ways. Since the cyber-physical layer of the system is connected to the cyber layer and (directly or indirectly) to the cyber environment, the effects of incidents at these layers could propagate all the way down to the physical layer. *Fig. 1* illustrates the typical components, actors and influences present in a wide range of CPS applications.

2.2 *UFoI-E concept*

The Uncontrolled Flows of Information and Energy (UFoI-E) concept integrates the safety and security frameworks from physical, control and computer systems in a common framework (Carreras Guzman and Kozine 2018). In this concept, Uncontrolled Flows of Information (UFoI) in the computer and control subsystems could lead - through system dependencies - to Uncontrolled Flows of Energy (UFoE) and cause harm to humans, assets or the natural environment. These dependencies between information and energy flows are particularly relevant in CPSs, where (semi)autonomous systems operate reacting in real-time to the physical world via sensors and actuators while also allowing cooperative control tasks with human operators.

From the notion that safety should be complemented with security, the UFoI-E concept considers the case of cyber threats (unintentional and deliberate) in the information domain cascading into safety hazards in the energy domain. Moreover, the UFoI-E concept also considers the case of physical attacks as deliberate sources of risk in the energy domain, in parallel to unintentional failures and deviations in physical components and in their system interactions. The UFoI-E concept incorporates the role of humans as well, conceiving them as sources of accidents and attacks at each domain. To avoid cases of UFoI and induced UFoE resulting in physical harm, the UFoI-E concept recommends the allocation of preventive and reactive barriers at each domain. *Fig. 2* illustrates this concept for combined safety and security analysis.

The UFoI-E concept incorporates the systems-theoretic perspective that safety and security are emergent properties of the system (Leveson 2011), (Ross, McEvilley, and Oren 2018) and can be compromised by dysfunctional interactions and flawed engineering design. Therefore, this concept requires a representation of the system to assist risk analysts in the identification and assessment of unintentional and deliberate risk sources.

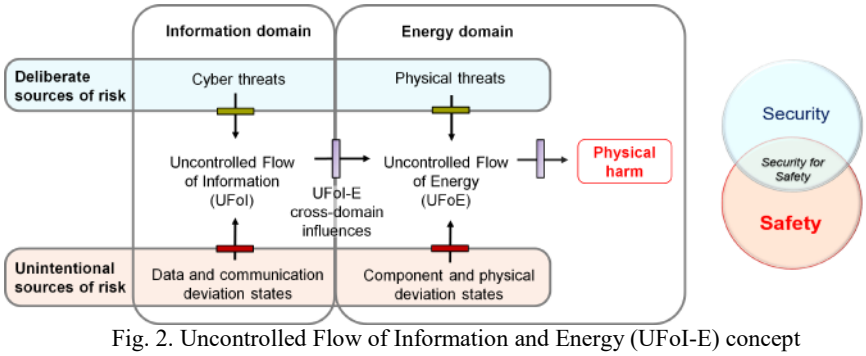

Fig. 2. Uncontrolled Flow of Information and Energy (UFoI-E) concept

Hence, by integrating the UFoI-E concept with the CPS master diagram, we find the possibilities of UFoI and UFoE interacting in feedback loops. In other words, the tight coupling between the system layers and the environment evidence the case that uncontrolled flows at any layer could cascade throughout the system in any direction and finalize at the region of safety hazards as UFoE.

The integration of the CPS master diagram and the UFoI-E concept constitutes the UFoI-E method for combined safety and security risk analysis of CPSs. This method begins from the representation of the CPS in terms of the CPS master diagram, conceptualizing the processes in the CPS in terms of system layers and environments with interacting flows of information and energy. Subsequently, the UFoI-E concept provides a framework to identify sources of unintentional and deliberate sources of risk with the potential to lead to physical harm as final consequence.

3. Case study: Safety and security in an autonomous surface vessel

The shipping industry, with its increased trend into digitalization and automation, is not exempt from cyber threats. In June 2017, the NotPetya ransomware attack disrupted several international companies. Among them, the shipping company Maersk reported expected losses of €350 million, with impacts in the global supply chain industry (NCSC 2018). More recently in July 2018, COSCO shipping lines reported a ransomware attack disrupting part of its operations in the Americas (World Maritime News 2018). A list of cybersecurity incidents that have caused alarm in the global shipping sector is available in (Corporate Allianz Global 2017).

In terms of safety-related risks, industrial recommended practices such as DNVGL-RP-0496 (DNV GL 2016) stress the potential of cyber-attacks to penetrate the system until reaching physical consequences. For example, targeted attacks could hijack the control of the ship and cause physical damages. The possibility of losing control of the ship functions due to remote cyber-attacks raises awareness of the influence of cyber risks in safety cases. Indeed, this potential for safety-related consequences goes beyond the service disruptions and economic losses produced by ransomware attacks, threatening the integrity of the ships and even the physical safety of the crewmembers.

3.1 *Autonomous vessel platform under analysis*

In the context of the Autosea project (NTNU n.d.), researchers and practitioners are working together to provide viable solutions for autonomous surface vessels (ASV) in different maritime applications. One of these applications, the Telemetron ASV, is equipped with a set of sensors (e.g. radar, automatic identification system) and navigation systems to facilitate autonomous operations at sea (Wilthil, Flåten, and Brekke 2017). Hence, the control system can drive the vessel according to a planned path by commanding the steering and propulsion system in autonomous mode. Moreover, a module of sensors provides inputs to the system regarding obstacles across the route, including other ships navigating and intersecting the planned route of the ASV in the near future. In these cases, a collision avoidance system (CAS) in the ASV can perform maneuvers in autonomous mode; avoiding the predicted obstacle trajectories and coming back to the predefined route after the collision with obstacles were prevented (Johansen, Perez, and Cristofaro 2016). *Fig. 3* shows the vessel Telemetron ASV platform.

Fig. 3. The Telemetron ASV navigating at sea (Hagen et al. 2018)

In this paper, we regard the CAS as a cutting-edge safety-related system. Indeed, the CAS

performs a safety function (collision avoidance) when the detected environmental conditions demand its activation. Currently based on radar sensors, Automatic Identification System (AIS), and target tracking algorithms, the control system detects the obstacles in the surroundings and predicts its future trajectory according to the evolution of its detected positions in time (i.e. with its linear speed and yaw rate). When the conditions predict a potential obstacle intersection with the own trajectory, the CAS modifies the route and commands the propulsion and steering system to implement the new course.

Standard traffic rules specified in the Convention on the International Regulations for Preventing Collisions at Sea (COLREGS) specify the control decisions that the CAS should implement in different scenarios. Therefore, according to different scenarios (e.g. head-on collision, crossing from right, crossing from left, overtaking) different collision avoidance functions are specified (Hagen et al. 2018). *Fig. 4* demonstrates the case of the Telemetron ASV implementing a collision avoidance function in the head-on collision scenario.

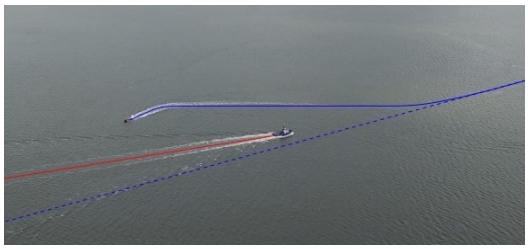

Fig. 4. Collision avoidance in head-on scenario: blue line dashed is Telemetron's initial route, blue line continuous is CAS maneuver, red line is the obstacle (Hagen et al. 2018)

4. Risk analysis and results using the UFoI-E method

4.1 *Collision avoidance system within its CPS context*

The objective of this analysis is to provide inputs to designers and stakeholders regarding the identification of risks and recommendations to evaluate the control architecture and technologies used in the current design of the ASV. Namely, this risk analysis aims at supporting the design and implementation of the CAS, preventing major injuries to people and assets while operating at sea in autonomous mode.

The CAS cannot be regarded as a traditional and isolated safety-related system, considering its deployment in the context of an autonomous vessel. The Telemetron ASV incorporates the CAS through the integration of various information technologies on-board (e.g. sensors, controllers, actuators) and remote (e.g. positioning systems, on shore monitoring stations) to control the physical processes guiding the vessel during operations at sea (i.e. propulsion and steering). Thus, the CAS is a safety-related system deployed in a CPS. *Fig. 5* describes the system architecture in the Telemetron ASV in terms of the CPS master diagram representation and presents a set of attack types potentially employed by external attackers. As part of a CPS, the CAS is subject to unintentional and deliberate sources of risk coming from interacting CPS layers and environments. Therefore, the CAS requires a combined safety and security risk analysis with a CPS approach.

Clearly, the goal of the CAS is to prevent collisions with obstacles and other ships. Hence, the hazardous event under control is a collision, i.e. uncontrolled flows of kinetic energy. In different CPSs, different energy sources are the safety hazards. Rausand (Rausand 2011) and several sector-specific references present a generic list of hazardous energy sources that analysts can use to explore systematically and discard the energy sources that are not within the scope of their system analysis. In the CPS master diagram, the hazards involved are found at the energy flows exchanged between the physical layer of the system and the physical environment. By analyzing the CPS master diagram, we can get a first overview of the safety and security risk sources.

In terms of unintentional motives, potential collisions may be associated to the failure of physical components in the vessel (e.g. motor failure) or to UFoI (e.g. inaccurate or missing inputs to the controller). Many uncertainties in the accuracy of the sensor readings and predictions of future trajectories may result in systemic errors of unintentional motive. Human operators interact with the system as remote supervisors in control rooms on shore, supervisors on-board or as physical operators in manual mode. Furthermore, the CAS is not isolated from the basic control system on the vessel, requiring an analysis of the dependencies between the safety function and the general-purpose components and control actions. Multiple controllers (human and automated) may lead to inadequate coordination and conflicting decisions, requiring conflict resolution protocols to prevent unsafe commands.

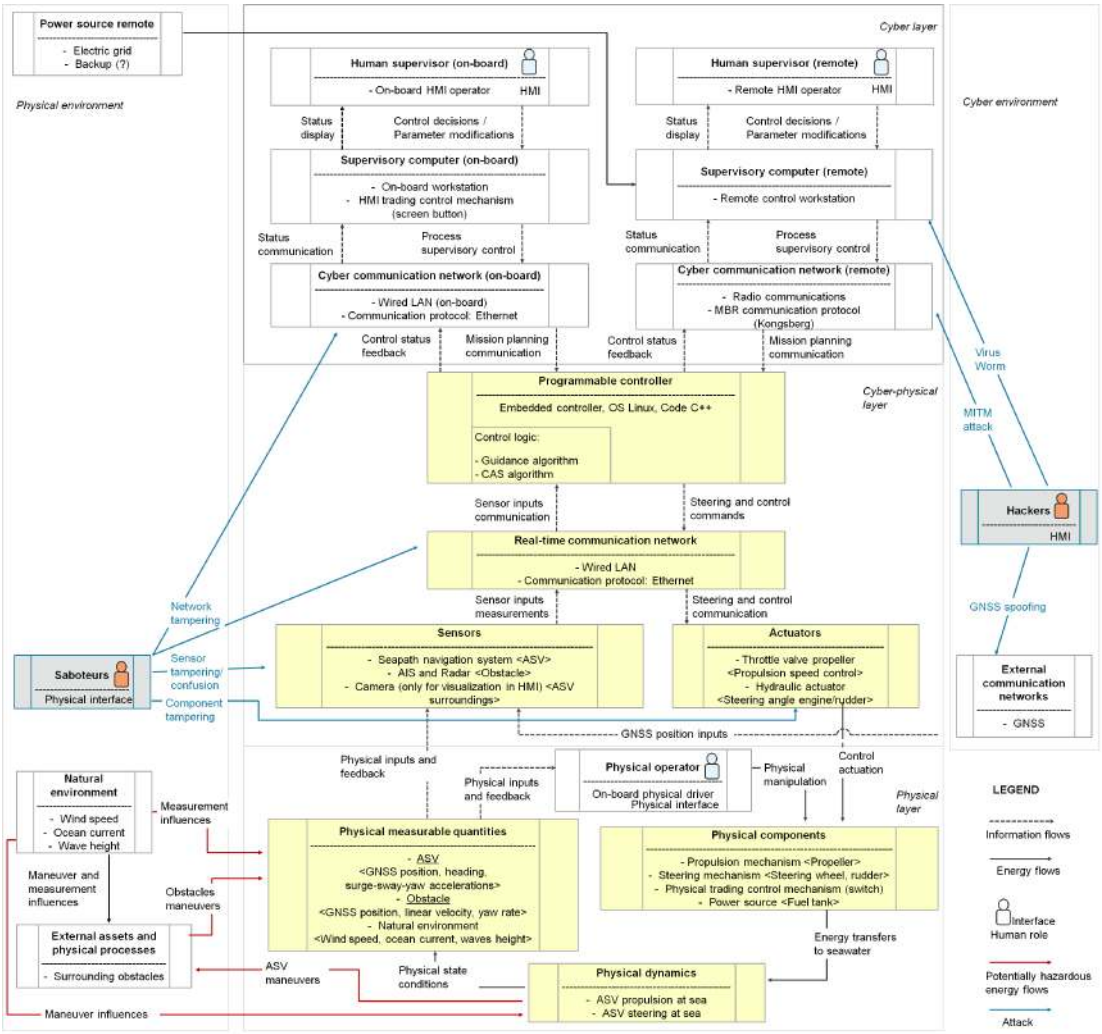

Fig. 5. The Telemetron ASV in CPS master diagram (CAS highlighted in yellow, potential attackers in grey)

In terms of cybersecurity threats, the use of standard protocols (e.g. global positioning system) make the system vulnerable to spoofing attacks, while the use of wireless communications (radio communications) could be subject to man-in-the-middle (MITM) attacks performed by remote hackers. The supervisory computers could be prone to virus or worm injections if they are not properly protected, potentially spreading throughout the system and infecting the controller. Considering physical security, saboteurs with physical access to the sensors and communication network on-board could tamper with the system. These sabotages could be performed in ways difficult to detect by operators or even by the control system itself in case that no proper feedbacks are set to check the status of the system before sailing (e.g. tamper alarms, periodic checks).

This first overview is purely the result of representing and analyzing the system using the CPS master diagram. However, to ensure a higher level of completeness in the risk identification process, a systematic risk analysis using the UFoI-E method traces back the flows of information and energy following the causal paths illustrated in the CPS master diagram. In the current version of the UFoI-E method, we trace back these scenarios using the conventions of fault tree analysis (FTA). Finally, a detailed fault tree has been constructed that is not displayed in the paper due to space limitations. The FTA is a useful technique that allows for quantification of the contributions from different causal paths leading to the UFoE. From probability measures provided to the basic events, we can evaluate the most critical paths and propose risk reduction measures.

5. Recommendations for safe and secure design of the ASV

The risk identification and analysis delineated in the previous sections lead to several recommendations for ensuring safety and security of the ASV. The recommendations can be grouped into (1) attack prevention, detection and protection, and (2) fault tolerance and robustness. This integrated safety and security analysis provides inputs for the system design. For example, for dealing with attacks we can extract the following recommendations:

- Secure radio communications with remote control center (e.g. message authentication, firewalls)
- Tamper resistance strategies for sensors and control network (e.g. security barriers, awareness alarms)
- Training of personnel to avoid malware injections at the cyber layer (e.g. via USB, e-mail phishing)
- Antivirus protection of supervisory computers

The above recommendations emphasize attack prevention, since it may be the only way to avoid adverse effects on the flow of information and energy that are difficult to detect. Furthermore, we recommend that fault tolerance and robustness strategies are built into the CAS. Specific fail-safe strategies can be implemented for detectable faults identified in the CPS master diagram and FTA. Moreover, deviation cases that are difficult to detect can be accounted for in the collision risk evaluation criteria of the CAS. For example, the collision risk evaluation of the CAS can be improved by including a probability measure of the occurrence of incidents and their consequences.

6. Conclusions

This paper described the Uncontrolled Flows of Information and Energy (UFoI-E) method for safety and security risk analysis of cyber-physical systems (CPSs). The integration of the safety and security frameworks of physical, control, and computer systems described in the UFoI-E method may provide inputs for new developments in safety and security standards, considering the comprehensive scope necessary to perform risk analysis of CPSs. We applied the UFoI-E method to analyze an autonomous surface vessel (ASV). Particularly, we analyzed the collision avoidance system (CAS) to prevent collisions while navigating at sea in autonomous mode. We proved the applicability of the UFoI-E method in this case, providing valuable insights for the design architecture of the ASV. In further work, we aim at providing a strategy to present a novel risk picture of the overall analysis, improving risk communication with decision-makers. Furthermore, a promising potential exists to use the UFoI-E method to analyze the control algorithm of the CAS and provide suggestions to the dynamic risk assessment of the ASV. Finally, we recommend a comparative study of the UFoI-E method with other safety and security analysis methods, validating the strengths and weaknesses of this method in this and other CPS applications.

Acknowledgement

The work of D. Kwame Minde Kufoalor is supported by the Research Council of Norway (NFR) through the projects 223254 and 244116/O70.

References

Aven, Terje. 2007. “A Unified Framework for Risk and Vulnerability Analysis Covering Both Safety and Security.” Reliability Engineering and System Safety 92 (6): 745–54. https://doi.org/10.1016/j.ress.2006.03.008.

Bolbot, Victor, Gerasimos Theotokatos, Luminita Manuela Bujorianu, and Evangelos Boulougouris. 2018. “Vulnerabilities and Safety Assurance Methods in Cyber-Physical Systems : A Comprehensive Review.” Reliability Engineering and System Safety 182 (September 2018): 179–93. https://doi.org/10.1016/j.ress.2018.09.004.

Carreras Guzman, Nelson H., and Igor Kozine. 2018. “Uncontrolled Flows of Information and Energy in Cyber-Physical Systems.” European Safety and Reliability Association Newsletter, 2018. http://www.esrahomepage.eu/filehandler.ashx?file=16438.

Carreras Guzman, Nelson H., Morten Wied, Igor Kozine, and Mary Ann Lundteigen. n.d. “Conceptualizing the Key Features of Cyber-Physical Systems in a Multi-Layered Representation for Safety and Security Analysis.” Systems Engineering, Under Review.

Chockalingam, Sabarathinam, Dina Hadziosmanovic, Wolter Pieters, Andre Teixeira, and Pieter van Gelder. 2013. “Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications.” In Critical Information Infrastructures Security. 8th International Workshop, CRITIS 2013. Revised Selected Papers: LNCS 8328. Vol.

8328. https://doi.org/10.1007/978-3-319-03964-0.

Corporate Allianz Global. 2017. "Safety and Shipping Review." 2017. https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Safety_Shipping_Review_2017.pdf.

DNV GL. 2016. "Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation." DNVGL-RP-0496.

Hagen, I B, D K M Kufoalor, E F Brekke, and T A Johansen. 2018. "MPC-Based Collision Avoidance Strategy for Existing Marine Vessel Guidance Systems." Proc. IEEE International Conference on Robotics & Automation (ICRA), 7618–23.

Humayed, A, J Lin, F Li, and B Luo. 2017. "Cyber-Physical Systems Security - A Survey." IEEE Internet of Things Journal 4 (6): 1802–31. https://doi.org/10.1109/JIOT.2017.2703172.

IEC. 2009. "IEC/TS 62443-1-1 - Industrial Communication Networks. Network and System Security. Part 1-1: Terminology, Concepts and Models."

———. 2010. "IEC 61508-1 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General Requirements."

ISO. 2011. "ISO 12100 - Safety of Machinery - General Principles for Design - Risk Assessment and Risk Reduction."

———. 2018. "ISO/TR 22100-4 - Safety of Machinery - Relationship with ISO 12100 - Part 4: Guidance to Machinery Manufacturers for Consideration of Related IT-Security (Cyber Security) Aspects."

Johansen, Tor A, Tristan Perez, and Andrea Cristofaro. 2016. "Ship Collision Avoidance and COLREGS Compliance Using Simulation-Based Control Behavior Selection with Predictive Hazard Assessment." IEEE Transactions on Intelligent Transportation Systems 17 (12): 3407–22. http://folk.ntnu.no/torarnj/colregs.pdf.

Kriaa, Siwar, Ludovic Pietre-Cambacedes, Marc Bouissou, and Yoran Halgand. 2015. "A Survey of Approaches Combining Safety and Security for Industrial Control Systems." Reliability Engineering & System Safety 139 (July): 156–78. https://doi.org/10.1016/j.ress.2015.02.008.

Langner, Ralph. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." IEEE Security and Privacy 9 (3): 49–51. https://doi.org/10.1109/MSP.2011.67.

Leveson, Nancy G. 2011. Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press. The MIT Press.

NCSC. 2018. "The Cyber Threat to UK Business: 2017-2018 Report." National Cyber Security Centre National Crime Agency. 2018. https://www.ncsc.gov.uk/cyberthreat.

NTNU. n.d. "Autosea: Sensor Fusion and Collision Avoidance for Autonomous Surface Vehicles." Norwegian University of Science and Technology (NTNU). Accessed November 18, 2018. https://www.ntnu.edu/autosea.

Pietre-Cambacedes, L., and M. Bouissou. 2013. "Cross-Fertilization between Safety and Security Engineering." Reliability Engineering and System Safety 110: 110–26. https://doi.org/10.1016/j.ress.2012.09.011.

Rajkumar, R., Insup Lee Insup Lee, Lui Sha Lui Sha, and J. Stankovic. 2010. "Cyber-Physical Systems: The next Computing Revolution." Design Automation Conference (DAC), 2010 47th ACM/IEEE, 0–5. https://doi.org/10.1145/1837274.1837461.

Rausand, Marvin. 2011. Risk Assessment: Theory, Methods, and Applications. John Wiley & Sons.

Ross, Ron, Michael McEvilley, and Janet Oren. 2018. "NIST Special Publication 800-160: Systems Security Engineering." https://doi.org/10.6028/NIST.SP.800-160v1.

Sun, Mu, Sibin Mohan, Lui Sha, and Carl Gunter. 2009. "Addressing Safety and Security Contradictions in Cyber-Physical Systems." Proceedings of the 1st Workshop on Future Directions in Cyber-Physical Systems Security (CPSSW' 09). http://cimic3.rutgers.edu/positionPapers/cpssecurity09_MuSun.pdf.

Wilthil, Erik F, Andreas L Flåten, and Edmund F Brekke. 2017. "A Target Tracking System for ASV Collision Avoidance Based on the PDAF." In Lecture Notes in Control and Information Sciences. Vol. 474. Springer. https://doi.org/10.1007/978-3-319-55372-6_13.

World Maritime News. 2018. "COSCO Shipping Lines Falls Victim to Cyber Attack." 2018. https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/.

Yampolskiy, Mark, Peter Horvath, Xenofon D. Koutsoukos, Yuan Xue, and Janos Sztipanovits. 2013. "Taxonomy for Description of Cross-Domain Attacks on CPS." Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems - HiCoNS '13, 135. https://doi.org/10.1145/2461446.2461465.

Zio, E. 2018. "The Future of Risk Assessment." Reliability Engineering and System Safety 177: 176–90. https://doi.org/10.1016/j.ress.2018.04.020.