Early combined safety - security Defense in Depth assessment of complex systems

Nikolaos Papakonstantinou[[1]](#footnote-2), Joonas Linnosmaa, Ahmed Z. Bashir, Timo Malm and Douglas L. Van Bossuyt

Key Words: Safety, Security, dependency model, early assessment, defense in depth, complex systems

SUMMARY & CONCLUSIONS

Safety and security of complex critical infrastructures is very important for economic, environmental and social reasons. The interdisciplinary and inter-system dependencies within these infrastructures introduce difficulties in the safety and security design. Late discovery of safety and security design weaknesses can lead to increased costs, additional system complexity, ineffective mitigation measures and delays to the deployment of the systems.

Traditionally, safety and security assessments are handled using different methods and tools, although some concepts are very similar, by specialized experts in different disciplines and are performed at different system design life-cycle phases.

The methodology proposed in this paper supports a concurrent safety and security Defense in Depth (DiD) assessment at an early design phase and it is designed to handle safety and security at a high level and not focus on specific practical technologies. It is assumed that regardless of the perceived level of security defenses in place, a determined (motivated, capable and/or well-funded) attacker can find a way to penetrate a layer of defense. While traditional security research focuses on removing vulnerabilities and increasing the difficulty to exploit weaknesses, our higher-level approach focuses on how the attacker’s reach can be limited and to increase the system’s capability for detection, identification, mitigation and tracking.

The proposed method can assess basic safety and security DiD design principles like Redundancy, Physical separation, Functional isolation, Facility functions, Diversity, Defense lines/Facility and Computer Security zones, Safety classes/Security Levels, Safety divisions and physical gates/conduits (as defined by the International Atomic Energy Agency (IAEA)) and international standards) concurrently and provide early feedback to the system engineer.

A prototype tool is developed that can parse the exported project file of the interdisciplinary model. Based on a set of safety and security attributes, the tool is able to assess aspects of the safety and security DiD capabilities of the design. Its results can be used to identify errors, improve the design and cut costs before a formal human expert inspection. The tool is demonstrated on a case study of an early conceptual design of a complex system of a nuclear power plant.

1. INTRODUCTION AND LITERATURE REVIEW
   1. *Security concepts in the nuclear domain*

Security in its broadest meaning is the degree of resistance to, or protection from harm. The overall site security as presented by the IAEA includes the Physical, Personnel, Information and Computer disciplines.

These disciplines of security interact and complement each other to establish a plant’s security posture. Failure in any of these disciplines of security can affect the other disciplines and cause extra requirements on the remaining system aspects [1]. In this paper, we abstract these disciplines into *physical security* including the “site”, “personnel” and “physical” disciplines and *cybersecurity* that includes the "computer" and "information" disciplines. In [2] security, Defense in Depth (DiD) is defined as the “*combination of successive layers of nuclear security measures for the protection of targets from nuclear security threats”.* It is identified as *“the primary means of preventing and mitigating the consequences of security breaches”* in [1]*.* This is very similar to the concept of ‘safety defense in depth’ and according to [3] the ‘safety defense in depth’ design of Instrumentation & Control (I&C) architectures incorporates concepts that may contribute positively to ‘security defense depth’ such as independence, redundancy and diversity.

The “Security Level” (SL) concept is relevant to the “Safety Class” of the nuclear safety domain and the “Security Integrity Level” of the machine safety domain. The Graded Approach (the level of security measures needs to match the threat probability and its expected impact) [2] called for the existence of different levels of prevention, detection, delay and response to malicious acts [3]. It is interesting that security levels are conceptualized differently by IEC 62443 [7] (4 levels, SL1 is the lowest level while SL4 is the highest) [4] compared to IAEA [1] (six levels, generic and Levels 1 to 5, where Level 1 is the highest and Level 5 is the lowest).

The “Facility function” is a security concept similar to the safety function. Facility functions are defined as “activities, actions, processes, and operations that are needed to ensure the safety and security of a facility” [5]. In the same way each safety function is assigned a safety class while the facility function is assigned to a security level [5].

* 1. *Computer and facility security zones*

The “security zone” is a concept similar to the safety defense line. Two kinds of security zones are being identified based on the international regulations: 1) the computer and 2) the facility security zone. The computer security zone is a concept used when “*logically or physically grouping computer systems that share common security requirements*” [3] occurs. The computer systems and networks belonging to the same zone require similar cybersecurity measures. Systems, which belong to the same zone, form an area for trusted internal communications. The facility security zone is a concept used to separate physical spaces/areas inside the plant from one another, so that the systems and components important to safety are protected, and access control and the control of goods traffic is possible [6]. Similar to computer security zones, the areas belonging to the same facility security zone should have similar requirements for physical security measures. The Finnish nuclear safety guide YVL A.11 [6] gives an example of implementation of five security zones located within another in growing order of strictness: site area, restricted area, plant area, protected area and vital area. Each cyber and physical security zone should be kept isolated and separated when feasible; however technical and physical control boundaries should still allow communication and flow of material between systems and the area within different zones [7]. Security zones need a way to have internal and external secure communication channels/gateways. Computer security zones use the concept of “Conduit”, while facility security zones traditionally use physical gates. “*A conduit is a particular type of security zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone*” [7]. Conduits are often technical countermeasures to prevent a higher security zone being compromised by a lower level zone by means of, for example, firewalls or antiviruses.Facility security zones are connected through physical barriers with access control. Physical gates can be e.g. locks or PIN codes. YVL A.11 states that each safety division (and security zone), separating redundant systems, should have a special physical gate, a secure emergency access route to the external environment.

Computer and facility security zones form networks or physical areas where systems or spaces have similar security requirements. Each of these zones is assigned a security level based on the attack probability and predicted impact [3, 7].All the systems assigned to a certain security zone need to fulfil the requirements given to the assigned security level. In our methodology, when we mention security level, we mean the achieved security level as defined in [7].

For human operators, Authorization levels allow assignment of access rights to persons working in different zones, making it possible to limit access to confidential systems and areas. The Two-person rule requiring at least two persons with the correct authorization to be present for a high security level activity is another way to either limit access of an individual to certain components or add redundancy to an activity involving the safety of the plant [3, 8].

* 1. *Mapping of concepts between safety and security DiD*

Within the security concepts, we have identified similarities to well-known safety DiD concepts. Security zones map to the defense lines of the safety DiD layers. Just as with the separation and strength of individual defense lines, the security zones need to be separated with gates and conduits to remove un-needed dependencies between higher and lower level zones. The same mapping could be done between security level and safety class. The objective of both concepts is to identify and set appropriate design and assurance requirements for the implementation of the target system or component. Also, a system of a certain safety class or security level is often required to interact only with systems of the same safety class or security level. The last example of a similarity is redundancy between safety components or functions to redundancy of security components or functions. Just like a high safety class function is required to be implemented with redundant systems, a high security level function is required to be implemented with redundant security arrangements, for example two-way authentication or the two-person rule.

1. Resilience, Survivability, towards a common safety and security model AND BACKGROUND

In past work, we studied the potential of using an early multidisciplinary model of a complex system to assess DiD capabilities [9] and generated a hybrid threat and fault tree demonstrating that threats can have an important safety impact to the plant [10]. This paper extends the multidisciplinary dependency metamodel used in past work with key security concepts to support a concurrent early safety and security assessment workflow for complex cyber physical systems.

Although safety and security have different foci, they overlap with each other and actions that advance one activity can have implications for the other [11]. They have a common purpose - the protection of people, society and the environment. Recently emerged global threats have raised attention to ensure adequate security at various safety-critical systems among critical infrastructure operators, regulators and international organizations. Nuclear power plants have been a particular focus of this effort. Over the years, nuclear power plants have benefitted from a sophisticated and comprehensive safety regime compared to security regimes, which are far less developed. There is interest to combine design and analysis methods to achieve both objectives in an optimal fashion. [11, 12]. In particular I&C systems have evolved during the last decades from analog and stand-alone equipment to digital and interconnected systems, thus exposing them to risks of cyberattacks as defined in IEC 62859] [12].

IAEA has recognized that there is a lack of a common international approach for combined safety and security modelling [3] and it is an active research topic. The key concepts that are being studied relevant to combined safety and security frameworks for modelling and assessment are *Resilience* and *Survivability*.

*Resilience* can be defined as “The intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances so that it can sustain required operations under both expected and unexpected conditions” [13] with the key aspects being the anticipation of, monitoring of, response to and learning from expected and unexpected conditions [13].

*Survivability* is part of resilience and can be defined as “the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents” [14]. Fisher et al. make the claim that while many times it is not possible to distinguish the cause of the event between a security attack and a safety failure, the system needs to be ready to survive (sustain vital functions) regardless [14]. Firesmith [15] studies information models related to security, safety and survivability while Goertzel [16] offers an overview of software survivability. [17] present three approaches for modelling and analysis of the survivability of smart infrastructures while [18] propose the Unified Modelling Language (UML) [19] profile called SecAM for security assessment in the context of survivability. [20] propose a model-driven method and a tool -MASDES- to assess the survivability requirements of critical systems, focusing on the security aspect. [21] provide a good overview and concepts definition of the resilience disciplines. Survivability, safety and security are part of resilience. Redundancy and diversity (typical DiD principles) are presented at the "resilience" level, above safety and security.

A plethora of research efforts on a combined safety and security approach demonstrate the interest in this direction. [22] proposes a method for managing the RAMS + S (Reliability Availability Maintainability Safety + Security) of complex systems. [23] focus on the nuclear domain and the cross-fertilizations between safety and security tools and methods.

Significant ongoing research activities focus on model-driven security engineering for industrial systems. An ontology-based framework for security decision support is presented in [24]. Ntalampiras [25] proposes a model-driven method for attack detection for critical infrastructures while [26] study the impact of security related events to safety systems. [27] developed an integrated model for safety and security requirements for facilitating certification processes. [28] research the relation between IEC 61784-3 (safe industrial automation networks) with the security concepts of IEC 62443 [7].

1. METHODOLOGY

This paper supports the early assessment of safety and security capabilities of early complex system architectures based on a multidisciplinary dependency model of the system. This research extends past work [9] focusing on the evaluation of safety DiD capabilities towards the concurrent assessment of security capabilities.

* 1. *Methodology overview - workflow*

The proposed method is based on model-driven engineering. A metamodel is developed to allow modelling of a multidisciplinary dependency model of the system (including process, automation, human factors, environment, power distribution and software aspects). This modelling can utilize a language like UML and in that case, the metamodel is a UML profile.

To support the security assessment of complex systems the UML profile proposed for safety assessment in [9] is extended here with security concepts of facility functions, security levels, authorization levels, computer and facility security zones, conduits and physical gates

The four steps of the proposed combined early safety and security assessment are:

Step 1: Develop the multidisciplinary dependency model of the system focusing on interdisciplinary connections (dependencies between disciplines).

Step 2: Add the known safety and security aspects (safety/security system components and attributes).

Step 3: A software tool automatically assesses the safety and security capabilities of the system based on a set of safety and security rules (this paper focuses on the security part, the safety aspect was addressed in [9]).

Step 4: Safety/security engineers and system engineers evaluate the feedback of step 3. Use the results to improve the system design. If changes are done, return to step 3.

* 1. *Security-related rules and verification process*

A list of security-related rules was extracted from the relevant regulations, which were able to be automatically reasoned by software based on the multidisciplinary early dependency model of a complex system:

Rule 1: Controls considered to be security-critical need to require two humans with the correct Authorization level in order to be actuated [3, 8]. Actuation panels with controls having the “TwoPersonRule” attribute set to true need to have the “PhysicalGate” stereotype applied (meaning that there is a physical access control mechanism) and they have to be linked to two humans with the correct Authorization level.

Rule 2: Between computer networks allocated to different Computer Security Zones there needs to be a “Conduit” gate. If the security level of the conduit is less than the endpoint computer zone, then the conduit should be marked as “Untrusted” [7]. There should be no direct connection between different computer security zones. Indirect connections need a conduit. If the conduit's security level is lower than the security level of the receiving computer network, the conduit should have the untrusted attribute set to true.

Rule 3: A secure gateway, a physical gate, with the “EmergencyExit” stereotype should be placed between each safety division and the external environment. This emergency access route needs to block unlawful use [6]. If a room is part of a safety division, an emergency exit physical gate should exist leading to the external environment.

Rule 4: Any connection between different Facility Security Zones needs a secure physical gate [6]. There should be no direct connection between different facility security zones. Indirect connections need to go through a physical gate.

Rule 5: Computer Security Zones and Facility Security Zones are assigned a Security Level. Computer device components that are members of a computer network allocated to a computer security zone and physical components located in a space that is part of a facility security zone need to have the same security level as the zone [3, 5]. There needs to be an assignment of security levels to facility and computer security zones. All component parts of a computer network allocated to a computer security zone or located to a space allocated to a facility security zone need to have that security level.

Rule 6: Humans also need to have a minimum Authorization Level according to the security level of the components they are interacting with and with the space they are in [3, 29]. All humans interacting with a computer network allocated to a computer security zone or located in a space allocated to a facility security zone or are otherwise interacting with a component of a specific security level need to have the appropriate Authorization Level.

Rule 7: Each facility function is assigned to one security level. The security level of the function should agree with the security level of the components mapped to that function [5]. System components allocated to facility functions need to have an appropriate security level as the function.

Rule 8: Each system should be located within a single facility security zone [5]. System components allocated to a system need to be in the same facility security zone.

1. CASE STUDY

The method is demonstrated on the case study of a spent fuel pool cooling system, presented in more detail in past work [9]. The model was extended with the needed security components and attributes before the automatic assessment tool checked the security rules (see the “*Methodology*” section).



Figure 1. Partial dependency diagrams from the case study modelling the environment (top), automation (left) and human factors (right)

* 1. *Case study description*

The spent fuel pool cooling system’s main function is to keep the temperature of the spent fuel of a Nuclear Power Plant at a safe level. Two redundant cooling loops and an emergency water injection system are used to achieve this goal. The process components are distributed in rooms across the levels/floors (rooms, doors, corridors, air ducts, water drains and staircases are part of the environment model). The system is operated by two operators and a supervisor and other humans are also involved e.g. for software development-distribution-maintenance, for process maintenance, etc. The human factors model was extended in [10] with internal and external security “Attackers”. Other aspects of the systems being modelled are the power distribution, the control automation hardware, the control software and the simple functional decomposition. The safety aspects of the system are presented in [9]. Due to space constraints, only partial dependency diagrams from a few system aspects can be presented in Figure 1.

The spent fuel pool cooling system model was extended in this paper with security information. Security levels were given to the components and the humans were assigned Authorization Levels. The emergency cooling system controls now need to satisfy the two-person rule to be operated. The computer networks for the emergency and the two main redundant cooling systems were assigned to computer security zones and the spaces of the plant (from the external environment to the vital areas) were assigned to facility security zones. Computer networks were now connected through conduits and the transition between facility security zones was through physical gates. Secure emergency access physical gates were introduced from the rooms belonging to the different safety divisions leading to the external environment. Facility functions were added in the functional model of the process. Omissions and errors in the security aspect were left in the model to test the security assessment tool.

1. Early assessment CASE study results

The prototype software tool introduced in [9] for safety DiD assessment was extended to support the method presented in this paper and check the set of security rules presented in the *Methodology* section based on the dependency model of the system under study. Examples of these results are:

Rule 1: One of the two operators required to control the emergency cooling system did not have high enough Authorization Level.

Rule 2: A connection between computer networks belonging to different computer security zones was through a communications channel not marked as “conduit”.

Rule 3: A room in the basement floor that was part of a safety division did not have an emergency exit to the external environment.

Rule 4: There were many connections between areas belonging to different facility security zones. Mainly the connections were through water drains and air ducts but also through other model aspects like the power distribution and the human factors.

Rule 5: Many system components did not have the correct security level according to the computer and facility security zone they were linked to, mainly because the security level was not set.

Rule 6: Many humans (operators, maintenance personnel, attackers etc.) did not have the correct security level according to the computer and facility security zone they were linked to.

Rule 7: Many system components did not have the same security level as the facility function they were allocated to, mainly because they did not have a security level set.

Rule 8: Components of a system were found to be allocated to more than one facility security zone. In some cases, this cannot be presented (e.g. when a cooling system has components in a vital area like the spent fuel pool, in a protected area with the majority of system components but also includes the site area (to get water to feed the secondary circuit of its heat exchanger)). Other model aspects like power distribution and control signal distribution components also crossed facility security zones.

This was a proof of concept case study and not a real system, so no further action is taken to address the assessment results. In a real engineering project, if issues are identified, there should be either a design iteration to address the identified issues and then a re-run of the tool or a justified decision as to why the issues can be treated as exceptions.

REFERENCES

[1] IAEA, "International Atomic Energy Agency, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17," ed. Vienna, 2011.

[2] IAEA, "International Atomic Energy Agency, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20," in Vienna, ed, 2013.

[3] IAEA, "International Atomic Energy Agency, Computer Security of Instrumentation, and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series, No. 33-T," ed. Vienna, 2018.

[4] TUViT. TUViT, Whitepaper Industrial Security based on IEC 62443. Available: https://www.tuvit.de/fileadmin/Content/TUV\_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf

[5] IAEA, "DRAFT: International Atomic Energy Agency, Computer Security Techniques for Nuclear Facilities," ed. Vienna, 2017.

[6] STUK, "YVL A.11 Security of a nuclear facility," ed, 2013.

[7] IEC/TS, "IEC/TS 62443-1-1:2009, "Industrial communication networks. Network and system security". Part 1-1: Terminology, concepts and models," ed, 2009.

[8] IAEA, "International Atomic Energy Agency, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G," ed. Vienna, 2015.

[9] N. Papakonstantinou, T. Tommila, B. O’Halloran, J. Alanen, and D. V. Bossuyt, "A Model Driven Approach for Early Assessment of Defense in Depth Capabilities of Complex Sociotechnical Systems," presented at the ASME IDETC/CIE Conference, Cleveland, Ohio, USA, 2017.

[10] N. Papakonstantinou, J. Linnosmaa, J. Alanen, A. Z. Bashir, B. O'Halloran, and D. L. Van Bossuyt, "Early hybrid safety and security risk assessment based on interdisciplinary dependency models," presented at the 65th RAMS 2019, Orlando, FL, USA, 2019.

[11] IAEA, "International Atomic Energy Agency. “The interface between safety and security at nuclear power plants”, A report by INSAG, INSAG-24," 2010.

[12] IEC, "“IEC 62859 Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity”, Edition 1.0," ed, 2016.

[13] E. Hollnagel, "How Resilient Is Your Organisation? An Introduction to the Resilience Analysis Grid (RAG)," presented at the Sustainable Transformation: Building a Resilient Organization, Toronto, Canada, 2010.

[14] D. Fisher, R. Linger, H. Lipson, T. Longstaff, N. Mead, and R. Ellison, "Survivable Network Systems: An Emerging Discipline, (CMU/SEI-97-TR-013)," Software Engineering Institute, Carnegie Mellon University1997.

[15] D. Firesmith, "Common Concepts Underlying Safety, Security, and Survivability Engineering, Technical Note CMU/SEI-2003-TN-033," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania2003.

[16] K. M. Goertzel and L. Feldman, "Software Survivability: Where Safety and Security Converge," in AIAA Infotech@Aerospace Conference, ed: American Institute of Aeronautics and Astronautics, 2009.

[17] A. Avritzer, L. Carnevali, H. Ghasemieh, L. Happe, B. R. Haverkort, A. Koziolek, D. Menasche, A. Remke, S. S. Sarvestani, and E. Vicario, "Survivability Evaluation of Gas, Water and Electricity Infrastructures," Electronic Notes in Theoretical Computer Science, vol. 310, pp. 5-25, 2015.

[18] R. J. Rodríguez, J. Merseguer, and S. Bernardi, "Modelling Security of Critical Infrastructures: A Survivability Assessment," The Computer Journal, vol. 58, pp. 2313-2327, 2015.

[19] Object Management Group (OMG). (2015). OMG Unified Modeling Language (OMG UML) specification. Available: http://www.omg.org/spec/UML/

[20] S. Bernardi, L. Dranca, and J. Merseguer, A model-driven approach to survivability requirement assessment for critical systems, 2016.

[21] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, vol. 54, pp. 1245-1265, 2010/06/01/ 2010.

[22] J. Link, K. Waedt, I. B. Zid, and X. Lou, "Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, Their Interoperability and Impact on Organizations: How to Manage RAMS + S (Reliability Availability Maintainability Safety + Security)," in ICRMS, 2018, pp. 185-191.

[23] L. Piètre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," Reliability Engineering & System Safety, vol. 110, pp. 110-126, 2013/02/01/ 2013.

[24] B. A. Mozzaquatro, R. Melo, C. Agostinho, and R. Jardim-Goncalves, "An ontology-based security framework for decision-making in industrial systems," in MODELSWARD, 2016, pp. 779-788.

[25] S. Ntalampiras, "Detection of Integrity Attacks in Cyber-Physical Critical Infrastructures Using Ensemble Modeling," IEEE TII, vol. 11, pp. 104-111, 2015.

[26] E. Ugljesa, H. Wacker, and J. Börcsök, "Modeling security aspects in safety environment," in 2011 7th International Conference on Electrical and Electronics Engineering (ELECO), 2011, pp. II-46-II-50.

[27] M. Brunner, M. Huber, C. Sauerwein, and R. Breu, "Towards an Integrated Model for Safety and Security Requirements of Cyber-Physical Systems," in 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2017, pp. 334-340.

[28] R. S. H. Piggin and H. A. Boyes, "Safety and security - A story of interdependence," in 10th IET System Safety and Cyber-Security Conference 2015, 2015, pp. 1-6.

[29] IAEA, "International Atomic Energy Agency, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4," ed. Vienna, 2007.

BIOGRAPHIES

Nikolaos Papakonstantinou, D.Sc. (Tech.)

VTT Technical Research Centre of Finland

P.O. Box 1000, FI-02044 VTT, Finland

e-mail: [nikolaos.papakonstantinou@vtt.fi](mailto:nikolaos.papakonstantinou@vtt.fi)

Dr. Nikolaos Papakonstantinou has a diploma in Electrical & Computer Engineering from the Univ. of Patras (Greece) and a doctorate degree in Information Technology in Automation from Aalto Univ. (Finland). Currently he is a senior scientist in the area of system modeling and simulations. His current interests include safety-security of complex systems and industrial applications of data mining.

Joonas Linnosmaa, MSC. (Tech.)

VTT Technical Research Centre of Finland

P.O Box 1300, FI-33101 Tampere, Finland

e-mail: [joonas.linnosmaa@vtt.fi](mailto:joonas.linnosmaa@vtt.fi)

M.Sc. Joonas Linnosmaa has a diploma in Safety & Process Engineering from Tampere Univ. of Technology (Finland). He works as a research scientist and his main field is Safety Critical System design and assessment. He is also interested in Data Driven approaches, like Machine Learning and Big Data. He is currently studying and implementing various Data Analysis, Processing and Mining methods.

Ahmed Z. Bashir, B. Eng., P. Eng., PM2

Department of National Defence, Attention: DNCS 4-6

101 Colonel By Drive, Ottawa, Ontario, K1A 0K2, Canada

e-mail: [ahmed.bashir@forces.gc.ca](mailto:ahmed.bashir@forces.gc.ca)

Ahmed Z. Bashir is the Vice-President of the Society of Reliability Engineers in Ottawa, Canada. He has been working on Naval Combat Systems for over 25 years and currently serves as a certified project manager and supervising engineer on unmanned and underwater warfare systems. Recent domains include submarine fire control, and submarine electronic warfare. His current interests lie in AI control and safety. He is a licensed Professional Engineer in Ontario.

Timo Malm, M.Sc. (Tech.)

VTT Technical Research Centre of Finland

P.O. Box 1300, FI-33101 Tampere, Finland

e-mail: [timo.malm@vtt.fi](mailto:timo.malm@vtt.fi)

Timo Malm has a Masters in Electrical Engineering from Tampere Univ. of Technology (Finland). Currently he is a senior scientist in the area of machinery safety and functional safety of machinery control systems. His current interests include functional safety and mutual safety and cybersecurity risks in machinery and industrial systems.

Douglas L. Van Bossuyt, PhD

Naval Postgraduate School

833 Dyer Road, Bullard Hall 218, Monterey, CA 93943, USA

e-mail: [douglas.vanbossuyt@nps.edu](mailto:douglas.vanbossuyt@nps.edu)

Dr. Douglas L. Van Bossuyt holds an Honors Bachelor of Science in Mechanical Engineering, an Honors Bachelor of Arts in International Studies, a Master of Science in Mechanical Engineering, and a Doctorate of Philosophy in Mechanical Engineering from Oregon State University (USA). He is currently an assistant professor in the Systems Engineering Department. His area of research focuses on risk and failure-informed conceptual design and trade-off study philosophies for complex systems.

1. Corresponding author. [↑](#footnote-ref-2)