A Process to Support Safety Analysis for a System-of-Systems

Stephan Baumgart*, Joakim Fröberg†, Sasikumar Punnekkat‡
* Volvo Autonomous Solutions, Eskilstuna, Sweden
Email: stephan.baumgart@volvo.com
† RISE Research Institutes of Sweden, Västerås, Sweden
Email: joakim.froberg@ri.se
‡School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
Email: sasikumar.punnekkat@mdh.se

***Abstract*—Autonomous vehicles grow importance in many domains and depending on the domain and user needs, autonomous vehicles can be designed as stand-alone solutions as in the automotive domain or as part of a fleet with a specific purpose as in the earth moving machinery domain. Contemporary hazard analysis methods primarily focus on analyzing hazards for single systems. Such an analysis requires knowledge about typical usage of a product, and it is evaluated among others if an operator is able to handle a critical situation. Each hazard analysis method requires specific information as input in order to conduct the method. However, for system-of-systems it is not yet clear how to analyze hazards and provide the required information. In this paper we describe a use case from the earth moving machinery domain where autonomous machines collaborate as a system-of-systems to achieve the mission. We propose a hierarchical process to document a system-of-systems and propose the use of model-based development methods. In this work we discuss how to utilize the provided details in a hazard analysis. Our approach helps to design a complex system-of-systems and supports hazard analysis in a more effective and efficient manner.**

***Index Terms*—Autonomy, System-of-Systems, Safety Analysis, Hazard Analysis**

I. Introduction

In the past decades the complexity of vehicles, airplanes, trains or heavy machinery has increased significantly, because of a higher utilization of software to provide new customer features. Some of these features support the human drivers or operators like assisting in parking a car (park assist), keeping the lane when driving (lane assist) or ensuring a safe distance to the vehicle in front (adaptive cruise control). We can recognize a trend in industry going from assisting features towards automating tasks of the operation with the intention to reduce the risk for human failure and increasing efficiency. Automation can focus on single vehicles, where the single vehicle is performing a task and collaboration with other systems is not required. In the earth moving machinery domain it is more common that various types of machines collaborate in a repetitive workflow. When automating such machines, the resulting workflows and possible collaborations and interactions must be analyzed thoroughly. Such collaborating systems can be seen as system-of-systems (SoS). When connecting single systems to a system-of-systems, a new level of complexity is added. A failure in constituent system A might not be critical for this system and therefore not identified as safety critical. By sharing this erroneous data through the communication network of connected constituent systems, this may lead to an unforeseen accident with constituent system B as described in [1]. Such systems-of-systems are growing their importance in the truck domain, where platooning of trucks is being explored to improve fuel efficiency [2] or automated vehicles transport material in off-road environments [3]–[5]. Developing system-of-systems and integrating automated vehicles add new dimensions of complexity to the already complex systems and processes. How to achieve safety when developing such a system-of-systems is not yet clear, since existing functional safety standards like ISO 26262 [6] or IEC 61508 [7] also do not explicitly cover system-of-systems.

In this paper, we provide guidance for practitioners on how to document a system-of-systems to aid the safety analysis of such a system. We propose a hierarchical process to document a system-of-systems and provide an example how model-based development practices can be utilized. The practices shown in this paper are based on our experience developing a safety-critical system-of-systems. We primarily focus on the concept stage as described in ISO 21839 [8]. In the concept stage, the system-of-interest shall be defined and analyzed, requirements shall be collected, and risks shall be identified, assessed and appropriate mitigation mechanisms shall be defined.

The paper is structured as follows. In section II we provide the background and related work in the area of system-of-systems and considering safety. As explained above, the provided guidance is related to our experience when designing a system-of-systems and we therefore provide a description of our use case in section III. In section IV we present our approach and describe the different phases. We conclude our paper in section V.

II. Background and Related Work

A. Safety Lifecycle

Developing safety-critical products requires to follow appropriate safety standards, where best practices and approved methods are embedded in a reference process. The term safety in general is related to the "absence of catastrophic consequences on the user(s) and the environment" [9]. The

usage scenarios and the included features of the targeted product need to be thoroughly analyzed to identify those situations, where users or bystanders are at risk to get injured or killed or other equipment or the environment can be damaged. This requires thorough analysis to identify what could potentially cause an accident to happen. Such causes can be for example failures in the components in the product or external influences. Analyzing potential failures in one of the embedded systems or the software running on the control units is covered under the term 'functional safety'. Functional safety is defined as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems" [6]. A hazard in this context is a "potential source of harm" [6], meaning that in a specific situation, the hazardous event, this hazard can lead to an accident. A typical example for such a standard is the automotive domain specific functional safety standard ISO 26262 [6]. This standard provides a framework for developing the embedded systems in a car. One part of the framework is a reference process containing process steps of development processes, production, operation, service and decommissioning and other supporting processes. The proposed development process starts with the concept phase, where an *Item* is defined. An item in the context of ISO 26262 is a "system or combination of systems, to which ISO 26262 is applied, that implements a function or part of a function at the vehicle level". An item is limited to a single vehicle and can be a feature like parking brake or steering. Requirements related to the item like the boundary, the targeted behavior seen from the driver's perspective, constraints and dependencies need to be captured. This input is used for conducting the hazard analysis and risk assessment (HARA) and determining the automotive safety integrity level (ASIL). These details are used throughout the development process and closure of the identified hazards need to be shown at the end of the development as part of the safety case, which includes arguments and evidence. This functional safety standard focuses on functions in a single vehicle, i.e., a single system. Clarification on how to develop a system-of-systems is not in the scope of ISO 26262.

B. Systems vs. System-of-Systems

In our work we focus on system-of-systems and therefore we provide a distinction between systems, on which the ISO 26262 focuses on and system-of-systems. ISO 26262 defines the term system as a "set of components or subsystems that relates at least a sensor, a controller and an actuator with one another" [6]. A more general definition of a system is provided in MIL-STD-882E [10]: "The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results." In the same standard the term system-of-systems is defined as "a set or arrangement of interdependent systems that are related or connected to provide a given capability" [10]. The standard ISO 21841 defines that a system-of-systems consists of a "set of systems or system elements that interact to provide a unique capability that none of the constituent systems can accomplish on its own" [11]. A constituent system in this context is an "independent system that forms part of a system of systems (SoS)" [11].

Various characteristics to highlight the differences between systems and system-of-systems have been listed in literature as for example:

- operational independence of the element [12], boundaries and interfaces [13]
- managerial independence of the elements [12], [13]
- evolution [12]
- emergent behavior [12]–[14]
- geographic distribution [12], operational focus [13]
- autonomy [14]
- belonging [14]
- connectivity [14]
- diversity [14]

A commonly accepted categorization of types of SoS has been proposed by Maier [15]. Maier is using the way a SoS is organized and managed as the parameter to differentiate them. He identifies three types of SoS: 1) Directed SoS, where a master system is coordinating the slave systems in an SoS. 2) Collaborative SoS, where the constituent systems may join a SoS to fulfill the goal of the SoS, and 3) a Virtual SoS, which have no central management or agreed purpose.

Axelsson [16] is providing an extension to the existing definitions by adding the states of the constituent systems, which has an impact if for example such a system is participating in a SoS or if it is not participating and passive with regards to the SoS.

C. Safety and System-of-Systems

In this section, we briefly discuss the literature focusing on safety in a system-of-systems. Hall-May and Kelly [17] utilize a case from the military domain and describe a system-of-systems using model-driven engineering methods and create a safety argumentation using the goal structuring notation (GSN) [18]. Alexander et. al [19] propose a simulation-based hazard analysis as a possibility to handle the complexity of interactions between constituent systems. Focusing on the interfaces and potential cascading failures in a system-of-systems, Redmond described the Interface Hazard Analysis method in [1], [20].

The compliance with existing functional safety standards like ISO 26262 [6] in the context of system-of-systems is described by Saberi et al. [21] through a platooning case from the truck domain and propose a tailored safety lifecycle. The authors highlight, that it is important to understand potential real live scenarios in order to be able to analyze the impact of failures and their potential cascading effect in this context. Axelsson and Kobetski [22] apply the system thinking approach STAMP [23] to analyze risks in a truck platooning case.

Compliance with functional safety standards requires considering critical scenarios during design-time. When self-adaptive collaborating systems are applied in a system-of-

systems and no central unit is used to coordinate the activities of the autonomous systems, not all constellations and situations can be considered during design-time. Instead, safety may need to be negotiated at run-time as presented in [24].

III. A Case from the Earth Moving Machinery Domain

We utilize the electric site research project [25] as a case for our work. In this project a fleet of automated guided vehicles (AGVs) called HX are used to transport pre-crushed material from a movable primary crusher to a stationary secondary crusher. Along with a fleet of autonomous HX, a human-operated wheel loader and a human-operated excavator are used for loading material on the HX. In our earlier works we have been analyzing safety in context of certain specified scenarios of this complex SoS [3], [4].

In Figure 1, a typical setup for an automated quarry site is presented. The automated guided vehicles follow predefined tracks on the site. In this configuration there are two alternative possibilities to load a HX with gravel. The first way is to utilize direct loading from the movable primary crusher (PCR), which is filled by an excavator (EXC). Alternatively, the HX can be loaded using a human-operated wheel loader (WL). In order to enable choosing which loading area is relevant, the empty HX wait at the main decision point (MDP) until they get a mission assigned by the fleet control server. A loaded HX transports the material to the stationary secondary crusher (SCR) and unload the contents there. Since the HXs are electrified, they require

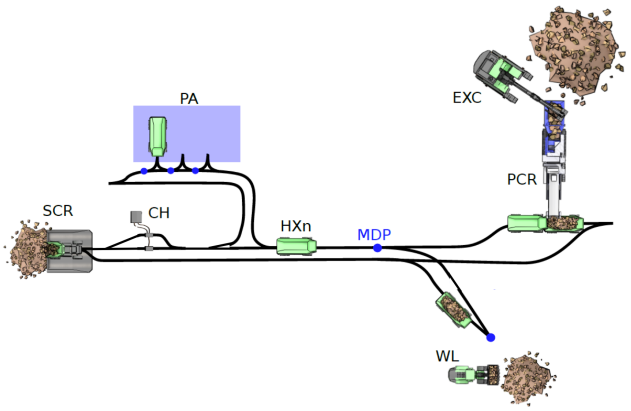

Fig. 1. Automated Quarry Site

charging of their batteries at the charging stations (CH).

Generally, a HX can either be controlled by a remote control or by a fleet control server as shown in Figure 2. While the remote control is maintaining a one-to-one connection and is directly controlling the vehicle movement, the fleet control server is providing vehicle-specific missions to the active HXs, which are interpreted and translated to movements by the on-board system of a targeted HX. The site operator is supervising the activities of the autonomous and human-operated vehicles and possible humans moving inside the restricted area.

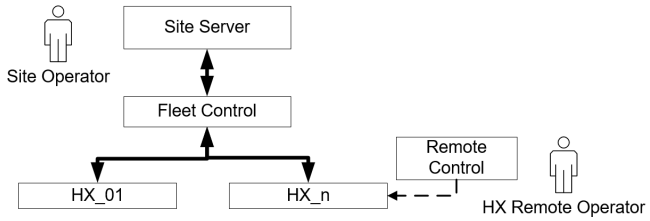

Fig. 2. Automated Quarry Site - Control Structure

The depicted quarry site case is one instance of such a site. When working with this research project we recognize the following dimensions that impact safety activities and argumentation:

1) Structure of SoS and constituent systems: The involved autonomous and human-operated machines, workflows and for example environmental conditions are specific for a site. Since workflows, tasks and environmental conditions may differ from one site to another, the safety and risk avoidance may differ as well. Accordingly, hazards and risks may be missed when reusing safety arguments.
2) Dynamicity at a site: The fleet of HX are operated in an outside and off-road environment with possible impact of changing weather conditions, which require adapting the workflow at a site. Furthermore, changes in the number of machines, changes in the production process, relocating loading and unloading spots and changing routes, may require revisiting the safety arguments.
3) Evolution of the SoS : Machines and systems may evolve over time with changed and adopted features or even new features. Such changes can for example be realized through software updates for improving the capabilities of a vehicle or adjusting the workflow to new conditions. Customer sites can be dynamic so that workflows and tasks evolve over time. This can impact the number and type of machines that are required. Usually, it is challenging to foresee how a site may evolve over time.

In order to be able to support the reuse of development artifacts and related safety analysis and safety concepts, a structured process on how to specify a system-of-systems supporting a safety analysis is necessary.

IV. The SafeSoS Approach

In this section we describe our approach called SafeSoS, which is including concepts for specifying a SoS and using those specifications for performing a safety analysis. We apply the hierarchical levels described by Axelsson [16] to provide a model-centric approach to design the system-of-systems. Axelsson is differentiating between macro analysis, where the scope and the context of the SoS is analyzed. This information is refined in the meso analysis, where information on how the constituent systems form is analyzed. In the micro analysis, the focus is on single constituent systems and how they contribute

to the overall SoS goal. We utilize this mindset to structure the information about the SoS.

In Figure 3 the SafeSoS process is shown with descriptions on macro level, meso level and micro level. For each of these levels we distinguish between information w.r.t. structure and behavior and discuss who typically can provide such information. All provided information and requirements on these levels are connected and used in the SoS safety analysis phase.

A. SoS Macro Level

The main goal of the SoS Macro Level of our process is to capture the boundary of the targeted system-of-systems, environmental characteristics and derive use cases and typical scenarios.

1) Macro Level - Structure: The constituent systems planned to be joining the SoS shall be listed. It is also necessary to consider other systems that could possibly enter the SoS operating zone. If for example the constituent systems are not aware of a vehicle entering the operating zone, there is a risk for fatal accidents. Especially, when considering automated vehicles to be part of the system-of-systems, an unknown vehicle entering the automated operating zone, may lead to unpredictable behavior. Another aspect to list is potentially exposed humans, such as informed people, for example those operating a constituent system or controlling the operation, and people that are not informed such as visitors or rescue teams. If possible, environmental conditions also need to be listed and how the capabilities of the SoS are influenced by different conditions. While icy tracks increase the braking distance for vehicles, hot weather conditions may lead to dust and reduced quality of sensor data.

2) Macro Level - Behavior: In the behavior level of the SoS Macro Level, the usage concepts of the SoS shall be described. This can contain use cases on how the SoS is used and how it can be operated. Typical scenarios need to be derived in order to be able to identify those scenarios, where for example humans are at risk. Additionally, the states of the SoS need to be described. In the above-mentioned quarry site, typical states can be morning startup, normal operations or evening shutdown. It is important to identify additional scenarios and use cases that can be relevant like emergency stop of all autonomous machines or their recovery to operation. In this context, the states of the SoS can provide an indication of possible critical situations and need to be captured.

In this initial phase it is useful to interview stakeholders and run brainstorming meetings with developers to understand the processes where the system-of-systems shall be applied. In such a brainstorming meeting, potential losses can be identified and rated to achieve a sorted list based on criticality. Based on the provided information, it can be analyzed which persons are at risk and which scenarios seem to be most critical. It is possible to derive hazard paths based on the identified potential losses.

B. SoS Meso Level

In the SoS Meso Level, the internal perspective of the SoS with focus both on the internal structure and interactions between the constituent systems are captured.

1) Meso Level Structure: The internal structure of the SoS will focus on which constituent systems are participating in a SoS, possible servers and through which channels they communicate. It is for example important to capture, if autonomous constituent systems shall communicate directly to each other or via a coordinating server. The structural dimension of the Meso Level will provide insights about the type SoS, as for example directed SoS or collaborative SoS [15].

2) Meso Level Behavior: In the behavior views of the SoS Meso Level the interaction between the involved humans and the constituent systems shall be described. By the help of this descriptions, possible human errors can be identified. As a second aspect, the interaction between the constituent systems shall be described. This may include additional information about complex messages that are shared between the constituent systems. By the help of these details, the propagation of possible failures can be studied. Finally, details about the states of the constituent systems and their dependencies shall be specified enabling identification of safe states as well as inconsistencies. An example on how the states of constituent systems depend on each other is depicted in Figure 4 using a SySML state chart diagram. In this example a remote control is used to connect to a HX and the server is deciding about the request. System Designers and safety engineers can provide the required information.

C. SoS Micro Level

The SoS Micro Level contains details about a single constituent system. This level also consists of structural and behavioral views.

1) Micro Level Structure: In the structural view of the SoS Micro Level, details about the internal structure of a constituent system are captured. It is important though to focus on those details related to the SoS. In our case it is necessary for example to document how the remote emergency stop feature, that shall stop all active machines at a site when initiated by the site operator, is realized inside the machine.

2) Micro Level Behavior: The behavior level of the SoS Micro level contains details about timing, states or messaging characteristics of a single constituent system with respect to the SoS it is integrated in. The states of the constituent system are directly connected to the states for the complete SoS as described on the SoS Meso Level.

For the Micro Level details, system developers can provide the relevant information and safety engineers may help that all safety related details are provided.

It is necessary to ensure sufficient traceability between the levels, for which we have used state machines. The use cases on SoS Macro Level for example are directly connected to the Human Interactions with SoS on SoS Meso Level.

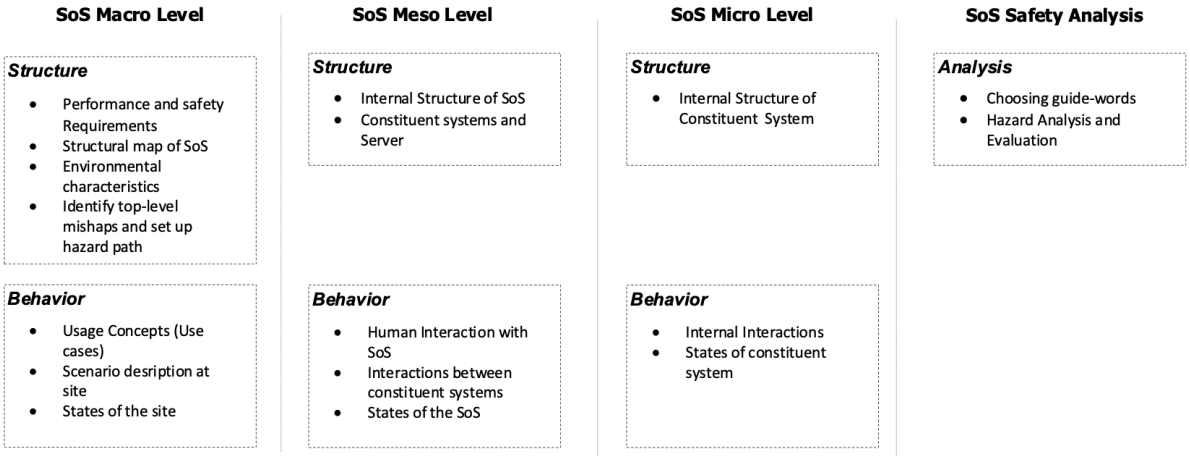

Fig. 3. SafeSoS: Safety Process to support System-of-Systems

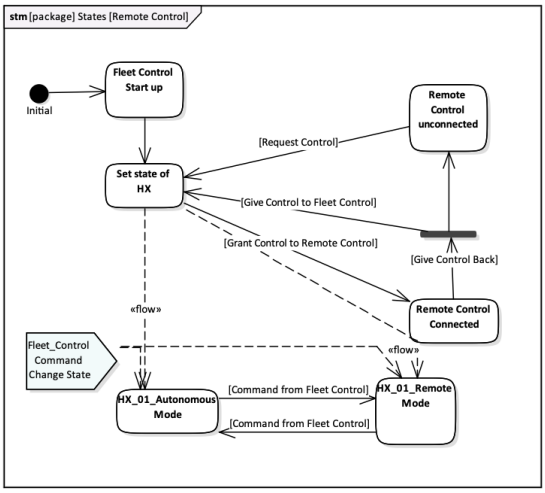

Fig. 4. State Chart - Remote Control Case

D. SoS Safety Analysis

In this section, we describe how a safety analysis for a SoS can be performed utilizing the information provided as part of the SoS specifications. As we described above, the possible humans at risk and possible critical scenarios are important information to understand where humans are at risk. The Meso Level is providing information about control structures, communication channels, timing aspects and potential safe states. The Micro Level in the scope of this paper is solely focusing on the states of a specific constituent system.

Guidewords help to identify critical situations and are commonly used in the literature on hazard analysis. In our work we have used the guidewords from the HAZOP methodology [26] as a starting point. Typical examples of guidewords are

- NO or NOT: This means, that a certain input is not provided or not received (indicating an 'Omission fault'). Depending on the SoS Level, a certain message is not provided by one constituent system or the SoS supervisor is not in an emergency stop when expected.
- MORE: Typically, this guideword would identify too long activation of a valve in the process industry (similar to a 'Commission fault'). In our case, different hazards may be detected using this guideword, depending on the SoS level. On Macro Level, MORE can characterize environmental changes or MORE speed of a specific constituent system. Another aspect that need to be considered is, that MORE constituent systems are used in an SoS, than it was started with for a day or than it was intended for which is indicating failures related to the dynamicity at the SoS.
- LATE: The intention of the LATE guideword is to identify those situations where controls or messages are provided too late (similar to a 'timing fault'). Again, depending on the SoS Levels, different scenarios can be identified. In the SoS Macro Level, the delayed identification of unauthorized personal at a quarry site, may lead to possible accidents when autonomous machines operate. On SoS Meso Level, delayed provision of the GPS position of an autonomous machine, may lead to higher uncertainties about current traffic situations.

The other HAZOP guidewords can also be used, but needs clarification about the meaning on the different SoS levels. It may also be necessary to tailor this list of guidewords to enable a full-fledged SoS safety analysis. From our experience, we added the guideword INCORRECT to our analysis (referring to a 'value fault'), to enable capturing the situation, when missions are sent from the server to the constituent systems. These messages may contain a list of positions and speed profiles for following the track. The message may be received on time and with correct length, but the contents may be wrong, which may lead the autonomous machine not operating as intended. The structural views of the SoS levels described above, help to find hazards related to malfunctioning systems

or components of the SoS. The behavior views help to find hazards related to the dynamicity of the SoS.

The results of the analysis performed in our case study was captured using a spreadsheet, where the structuring was pivoted based on use cases and scenarios. The classification helped to derive solutions during development to reduce the risks and provide evidence of mitigation implemented. The spreadsheet was generated in consultation with the design team as well as safety engineers, which resulted in identification of many potential risks (such as, remote control take over), which might have been overlooked otherwise. For individual hazard analysis we have used common methods like FMEA [27] as well as conformance with associated SIL [7]/ASIL [6] requirements. During this process, we also became aware of the many aspects of relevance which demand a more integrated tool-oriented approach for guiding such a safety analysis. Our planned works include development of a tool which can help in capturing essential information at each levels, connect them as well as have an intuitive user interface to the design/safety team. Having inter-operability by providing hooks to other detailed methods of relevance is also planned.

V. Conclusions

The existing hazard analysis methods focus on analyzing hazards for single systems. For the analysis, the usage of the final product needs to be known or assumed and therefore knowledge about application scenarios is essential. Each hazard analysis method requires specific information as input in order to conduct the method. For system-of-systems, how to specify the requirements, capture the essential safety relevant information and analyze hazards, still remain as an open and challenging research domain.

In this paper, we described a case from the earth moving machinery domain where autonomous machines collaborate and form a system-of-systems to meet the mission objective. We described an approach to document system-of-systems and show how the information is used for performing hazard analysis of SoS using guidewords. In the future, we plan to extend our approach and establish the connections and traceability to the individual machine's safety analysis.

Acknowledgments

The authors acknowledge the funding support received for this research from the KKS-funded ITS-EASY Post Graduate School for Embedded Software and Systems and the SUCCESS Project supported by the Assuring Autonomy International Programme (AAIP), a partnership between Lloyd's Register Foundation and the University of York.

References

[1] P. J. Redmond, "A System of Systems Interface Hazard Analysis Technique," Master's thesis, 2007. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a467343.pdf

[2] S. Tsugawa, S. Jeschke, and S. E. Shladovers, "A review of truck platooning projects for energy savings," *IEEE Transactions on Intelligent Vehicles*, vol. 1, no. 1, pp. 68–77, 2016.

[3] S. Baumgart, J. Froberg, and S. Punnekkat, "Analyzing hazards in system-of-systems: Described in a quarry site automation context," in *2017 Annual IEEE International Systems Conference (SysCon)*. IEEE, 4 2017, pp. 1–8.

[4] ——, "Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site," in *2018 IEEE International Systems Engineering Symposium (ISSE)*, no. 4. IEEE, 10 2018, pp. 1–8. [Online]. Available: http://www.es.mdh.se/publications/5246-https://ieeexplore.ieee.org/document/8544433/

[5] S. Baumgart, J. Fröberg, and S. Punnekkat, "A State-based Extension to STPA for Safety-Critical System-of-Systems," in *4th International Conference on System Reliability and Safety*, 11 2019. [Online]. Available: http://www.es.mdh.se/publications/5674-

[6] International Organization for Standardization, "ISO 26262:2018 - Road vehicles – Functional safety," 2018.

[7] International Electrotechnical Comission, "IEC 61508:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," 2010.

[8] International Organization for Standardization, "ISO/IEC/ IEEE 21839 -Systems and software engineering - System of systems (SoS) considerations in life cycle stages of a system," 2019.

[9] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *Dependable and Secure Computing, IEEE Transactions on*, vol. 1, no. 1, pp. 11–33, 2004.

[10] United States Department of Defense, "MIL-STD-882E," Washington, DC, USA, 2012.

[11] International Organization for Standardization, "ISO/IEC/IEEE 21841 Systems and software engineering — Taxonomy of systems of systems," 2019.

[12] M. W. Maier, "Architecting Principles for Systems-of-Systems," *INCOSE International Symposium*, vol. 6, no. 1, pp. 565–573, 1996.

[13] J. S. Dahmann and K. J. Baldwin, "Understanding the Current State of US Defense Systems of Systems and the Implications for Systems Engineering," in *2008 2nd Annual IEEE Systems Conference*, 2008.

[14] J. Boardman and B. Sauser, "System of Systems - The meaning of of," *Proceedings 2006 IEEE/SMC International Conference on System of Systems Engineering*, vol. 2006, no. April, pp. 118–123, 2006.

[15] M. W. Maier, "Architecting principles for systems-of-systems," *Systems Engineering*, vol. 1, no. 4, pp. 267–284, 1998.

[16] J. Axelsson, "A Refined Terminology on System-of-Systems Substructure and Constituent System States," *2019 14th Annual Conference System of Systems Engineering (SoSE)*, pp. 31–36, 2019.

[17] M. Hall-May and T. Kelly, "Using Agent-based Modelling Approaches to Support the Development of Safety Policy for Systems of Systems," *Proceedings of the 25th International Conference on Computer Safety, Reliability and Security (SAFECOMP '06)*, pp. 330–343, 2006.

[18] T. P. Kelly, "Arguing Safety – A Systematic Approach to Managing Safety Cases," Ph.D. dissertation, University of York, 1998.

[19] R. Alexander, D. Kazakov, and T. Kelly, "System of Systems Hazard Analysis Using Simulation and Machine Learning," pp. 1–14, 2006.

[20] P. J. Redmond, J. B. Michael, and P. V. Shebalin, "Interface hazard analysis for system of systems," in *2008 IEEE International Conference on System of Systems Engineering*. IEEE, 6 2008, pp. 1–8. [Online]. Available: http://ieeexplore.ieee.org/document/4724202/

[21] A. K. Saberi, E. Barbier, F. Benders, and M. Van Den Brand, "On functional safety methods: A system of systems approach," in *12th Annual IEEE International Systems Conference, SysCon 2018 - Proceedings*, 2018, pp. 1–6.

[22] J. Axelsson and A. Kobetski, "Towards a risk analysis method for systems-of-systems based on systems thinking," in *2018 Annual IEEE International Systems Conference (SysCon)*. IEEE, 4 2018, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/8369501/

[23] N. G. Leveson and J. P. Thomas, *STPA Handbook*, 2018.

[24] D. Schneider and M. Trapp, "Runtime Safety Models in Open Systems of Systems," *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. 455–460, 2009. [Online]. Available: http://ieeexplore.ieee.org/document/5380438/

[25] Volvo Construction Equipment, "Electric Site Project." [Online]. Available: https://www.volvoce.com/global/en/news-and-events/news-and-press-releases/2018/carbon-emissions-reduced-by-98-at-volvo-construction-equipment-and-skanskas-electric-site/

[26] International Electronical Commission, "IEC 61882:2001 Hazard and operability studies (HAZOP studies) — Application guide," 2001.

[27] C. Ericson, *Hazard analysis techniques for system safety*. Wileys, 2015.