How to Analyze the Safety of Concepts for a System-of-Systems?

Stephan Baumgart*, Joakim Fröberg[†‡], Sasikumar Punnekkat[‡]
* EES Architecture Department, Volvo Construction Equipment, Eskilstuna, Sweden
Email: stephan.baumgart@volvo.com
[†] Safety Integrity, Västerås, Sweden
Email: joakim.froberg@safetyintegrity.se
[‡]School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
Email: sasikumar.punnekkat@mdh.se

***Abstract*—Developing safety-critical products like cars, trains, or airplanes requires rigor in following development processes, and evidence for product safety must be collected. Safety needs to be considered during each development step and traced through the development life cycle. The current standards and approaches focus on single human-operated products.**

The technical evolution enables integrating existing products and new autonomous products into system-of-systems to automate workflows and production streams. Developing safety-critical systems-of-systems requires similar processes and mapping to safety-related activities. However, it is unclear how to consider safety during different development steps for a safety-critical system-of-systems. The existing hazard analysis methods are not explicitly mapped to developing a system-of-systems and are vague about the required information on the intended behavior. This paper focuses on the concept phase for developing a system-of-systems, where different technical concepts for a specific product feature are evaluated. Specifically, we concentrate on the evaluation of the safety properties of each concept. We present a process to support the concept phase and apply a model-driven approach to capture the system-of-systems' relevant information. We then show how this knowledge is used for conducting an FMEA and HAZOP analysis. Lastly, the results from the analysis are mapped back into the sequence diagrams. This information is made available during the next development stages. We apply the method during the concept phase for designing an industrial system-of-systems. Our approach helps to design complex system-of-systems and supports concept evaluation considering the criticality of the concept under consideration.

***Index Terms*—Hazard Analysis and Risk Assessment, System-of-Systems, Autonomous Machines, Safety, Concept Phase**

I. Introduction

Industrial development of products like cars, construction equipment machines, or trains requires rigorous development processes based on paradigms like V-Model, Spiral model, or Waterfall model. These paradigms visualize required development steps and their relation to verification activities. Process maturity models like Capability Maturity Model Integration (CMMI) [1], and the Software Process Improvement and Capability Determination (SPICE) [2] provide guidance to improve established development processes to show repeatability and quality management. Developing safety-critical products requires following the requirements of appropriate safety standards. For embedded systems, functional safety standards like ISO 26262 [3] or IEC 61508 [4] describe requirements on the development process. Typically, the required processes of the standards are tailored to the product's needs and the existing development and verification processes.

One crucial phase is the concept study, where various concepts are derived for a specific product function. Depending on the technical solution, new risks may be introduced. Accordingly, each concept must be evaluated from the technical but also from the safety perspective. For safety-critical products, hazard analysis methods like Preliminary Hazard Analysis (PHA) [5] or Hazard and Risk Assessment (HARA) [3] are conducted to evaluate the criticality and risk of different concepts. These processes and methods are standard practices for today's industrial development of safety-critical human-operated cars and machines.

The technical evolution enables multiple systems to be connected to a system-of-systems to provide new features that cannot be realized by a single system alone. Specifically, automation of systems like cars or machines allows providing new features when interacting in a system-of-systems. However, it is challenging to ensure safety for a system-of-systems as both standards and processes are not capable of fully identifying all hazards and hazardous events during development. When designing a system-of-systems, identifying all concepts and analyzing them is essential. In our work, we focus on the earth-moving machinery domain, specifically where autonomous machines are used in quarry sites as described in our previous work [6], [7]. In this paper, we describe an approach where the behavior of a system-of-systems is documented using SysML Sequence Diagrams. This information is transferred automatically to feed to FMEA and HAZOP analysis.

The paper is structured as follows. In section II we describe the background and related work used for this paper. We briefly describe the industrial case we studied in section III. Our approach to safety evaluation concepts for a system-of-systems is presented in section IV. We analyse our approach in section V and conclude our paper in section VI.

II. Background and Related Work

In this section, we describe the related work and the background to this paper.

A. Hazard Analysis Methods

A safety function is of a product "whose failure can result in an immediate increase of the risk(s)" [8].As a first step, the demanded features and functions of the product must be listed. In the second step, hazard analysis is conducted to identify product related hazards caused by for example sharp edges at a machine, by vibration or noise, or failures of the embedded systems. A hazard in the context of product safety is therefore defined as a "potential source of harm" [8]. However, to enable the identification of all potential sources of harm, the information must be made available. Additionally, knowledge about system states and environmental conditions is essential when a hazard is defined as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss." [9] When specific technical areas are in focus, the term hazard may be defined together with causes. The automotive domain functional safety standard ISO 26262 is defining a hazard as a "potential source of harm caused by malfunctioning behavior of the item" [3].

However, it is unclear how a system-of-systems shall be analyzed and which hazards are specific for such complex systems.

Many hazard analysis methods are applied in today's industrial development processes. Hazard analysis methods such as Preliminary Hazard Analysis (PHA), Hazard and Operability Analysis (HAZOP), Fault Tree Analysis (FTA) [10], and Failure Mode and Effect Analysis (FMEA) are typical well-established examples. In the scope of this work, we focus on FMEA and HAZOP, due to their capability find and evaluate component failures and provide guidewords for identifying process-related failures. Both dimension are essential when designing a system-of-systems with complex interactions.

A widely applied method is the Failure Mode and Effect Analysis (FMEA) [11], [12]. There are various types of FMEA, such as Process FMEA, where failure modes in processes are identified, and Design FMEA, where the design elements and components are analyzed. A failure mode of a component clarifies how this component may fail. The effect is corresponding to the consequence of the failure on the product level, for example, risks for a product customer.

The Hazard and operability studies (Hazop) [13], [14] is a method that was developed for identifying hazards related to the complex process in chemical factories. In comparison to FMEA, which is focusing on components, HAZOP is applicable for interactions. For this purpose, guidewords are available to structure the analysis and support the analysis team.

Generally, the complexity of a system-of-systems makes it challenging to identifying hazards. Additionally, the potential causes related to the interaction and interoperability of constituent systems need to be understood. Redmond [15] provides a classification of system-of-system hazards, which helps to distinguish types of hazards to be considered for a system-of-systems. The author argues that potential accidents (mishaps) related to a system will remain the same when integrating this system into an SoS. However, the causes may differ when integrating the system into an SoS. Therefore, the author distinguishes between single system hazards related to a specific system in the SoS and emergent hazards related to the integration into an SoS. Emergent hazards relate to the emergent behavior in an SoS and are divided into interoperability, reconfiguration, and integration hazards. Integrating systems into a system-of-systems may cause hazards related to the predefined interfaces, the shared resources, or the physical space where the constituent systems operate.

B. System vs. System-of-Systems

Since our focus is on system-of-systems, we now try to distinguish between systems and system-of-systems. A general definition of a system provided by the MIL-STD-882E [16] is: "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" [16]. 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" [17]. A constituent system in this context is an "independent system that forms part of a system of systems (SoS)" [17].

C. Model-based Approaches for System-of-Systems

Model-based engineering is applied in the industry for developing single complex systems. Various approaches for utilizing model-based formalism for specifying system-of-systems have been proposed in the research community. Mori et al. [18] utilize SysML to document the system-of-systems. Because of the complexity of a system-of-systems, the authors use different viewpoints, i.e., using different SysML diagram types. However, the authors do not consider supporting a hazard or safety analysis when designing a system-of-systems. Utilizing model-based development for safety analysis has been discussed by Guiochet et. al [19]. The authors apply UML diagrams to model the behavior of a medical robot. In addition, they use sequence charts, derive an error message model, and feed this information into an FMEA. Hall-May and Kelly [20] study multi-agent system design methods capturing the capabilities of constituent systems. Their purpose is to define rules and policies for the system-of-systems to avoid unintended emergent behaviors. The interaction between the constituent systems is essential in this context.

Apart from focusing on safety for a system-of-systems, the communicating constituent systems are vulnerable to cybersecurity threats. El Hachem et al. [21] propose an extension to SysML to support the awareness of possible security breaches when designing a system-of-systems.

III. Case Study - Mine Automation

We utilize the electric site research project [22] as a case for our work. This research project uses a fleet of automated guided vehicles (AGVs) called HX to transport pre-crushed material from a movable primary crusher to a stationary secondary crusher in an open-surface mine. Along with a fleet of autonomous HX, a human-operated wheel loader and a human-operated excavator are used to load the HX.

In Figure 1 the involved systems and human operators are presented. The Site Operator supervises the quarry site from a control room using displays connected to the Site Server. The Site Server aims to act as an interface between human-operated machines and the fleet of HX. The Fleet Control system controls the fleet of HX, containing functions for traffic management, setting missions for the active HX, and keeping track of each HX's status. The constituent systems at the site depend on a functioning and reliable wireless network. Depending on the targeted production at the quarry site, up to eight HX machines can be active simultaneously. An HX can also be manually operated using the remote control. This is necessary to, for example, start production or to remove an HX for maintenance purposes. The fleet of HX connected to the Fleet Control can be stopped by the Site Operator using an Emergency Button in the control room. Likewise, the Remote Control Operator can stop the connected HX using an emergency button on the remote control. Which operator can stop an HX is depending on which controller is connected to the particular machine.

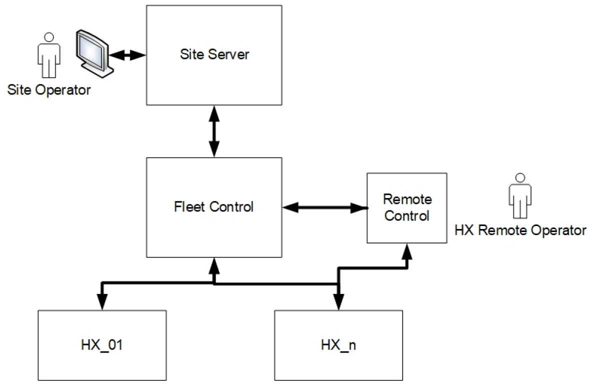


Fig. 1. Use Case: Remote Control of HX

Specifically, we are looking at a scenario where an HX is autonomously operated with commands received from the Fleet Control. The HX shall be removed from the fleet and set into manual mode to be operated by the remote control. There are different concepts possible how this can be technically realized.

This scenario needs to be thoroughly analyzed, and different concepts may lead to different risks. Typical accidents we foresee are

- Accident1: Fatal accident with human
- Accident2: Material damage.

The situations (hazards) we foresee for this scenario

- Hazard1: *Unintended propulsion of HX*
  An HX starts driving unintended because of a failure. This may lead to Accident1 and Accident2.
- Hazard2: *Unintended Steering of HX*
  Similar to Hazard1, the unintended steering of an HX can lead to critical accidents.
- Hazard3: *Unexpected HX connected to Remote Control*
  In comparison to Hazard1 and Hazard2, where we assume that the correct HX is connected for manual operation, Hazard3 covers the case that the wrong HX responds to the manual operation commands.

It needs to be analyzed how a malfunctioning constituent system or communication failure may lead to those accidents. The results from this analysis will guide to design of the system-of-systems appropriately.

Disconnecting the HX too early from the Fleet Control may leave the HX in an undefined state. Connecting too early may also lead to states of undefined behavior, where two controllers control the HX simultaneously.

IV. SafeSoS - Concept Evaluation

This section describes an approach to specify the interaction between the constituent systems in a system-of-systems. Model-based systems engineering is providing many different possibilities to capture the behavior. We started with textual written use cases and tried Activity Diagrams, Use Case Diagrams, and Sequence Diagrams. Additionally, we applied formal methods such as Petri Nets [23]. We have proposed a process called SafeSoS [24], where we suggest documenting an SoS using three abstraction levels: SoS Macro Level, SoS Meso Level, and SoS Micro Level. The details provided on each level are used in a safety analysis. This work focuses on the SoS Meso Level, where the interactions between the constituent systems are described.

A. Step 1 - Creating Concepts

At first, we exemplify how the change of control for an autonomous machine can be technically solved. In Figures 2 and 3 different communication concepts between the HX Remote Operator, the Fleet Control, the Site Server with the Site Operator and the targeted HX are shown.

Concept1 In Concept 1, the Remote Control is directly communicating with the Fleet Control. Then the HX receives the command from Fleet Control to be set into manual mode start listening to commands from Remote Control.

Concept2 In Concept 2, the Remote Control is directly communicating with the targeted HX. The HX is then requesting a status change at the Fleet Control.

In both cases, the Site Operator can set the status for an HX, which may complicate things additionally.

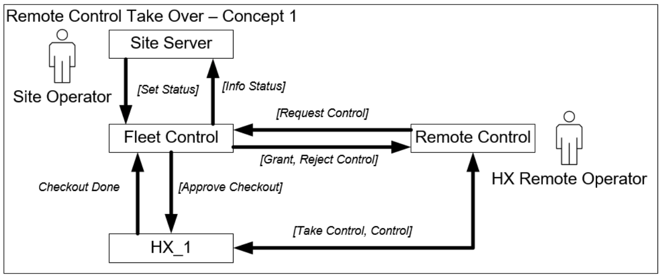


Fig. 2. Remote Control Take Over - Concept 1

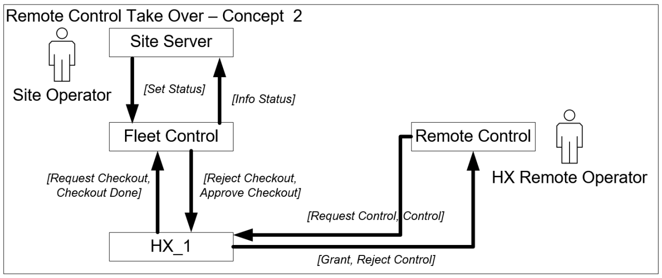

Remote Control Take Over – Concept 2
Site Server
Site Operator
[Set Status]
[Info Status]
Fleet Control
Remote Control
HX Remote Operator
[Request Checkout, Checkout Done]
[Reject Checkout, Approve Checkout]
[Request Control, Control]
HX_1
[Grant, Reject Control]

Fig. 3. Remote Control Take Over - Concept 2

Timing plays a vital role in this take-over of control scenario. Timing and order of commands are not visible in the concept descriptions shown in Figures 2 and 3. It shall not be possible that an HX remains in an undefined state if messages are lost or delayed.

B. Step 2 - Derive Sequence Diagrams

As a second step, we transfer the concepts to SysML sequence diagrams.

Sequence diagrams utilize swim lanes for depicting involved systems, components, or humans depending on the diagram's purpose. The communication between elements is visualized using lines with arrows indicating the direction of the message from a sender to a receiver.

We found sequence diagrams most suitable for our needs to provide input for a hazard analysis on concepts for the SoS Meso Level. Our purpose for the concept phase is to get a general idea of how the interaction between the systems may be designed. We set up the following rules for modeling the sequence diagrams on the SoS Meso Level.

1) Only the constituent systems of the system-of-systems shall be documented as swim lanes.
   Therefore, no subsystems, electric components, or software components shall be part of these sequence diagrams.
2) The communication between the constituent systems shall be reduced to the essential.
   There is a tendency among engineers to provide as much detail as possible. However, this would increase the complexity of the sequence diagrams and, therefore, efforts for the analysis would increase. These details are necessary during later stages, but finding the right abstraction level for analyzing concepts is vital to keep the efforts to a reasonable level.

We provide sequence diagrams for both concepts in Figure 4 and 5.

Concept 1 In concept1, the Remote Control is directly communicating with the Fleet Control Server. The details of this communication are presented in Figure 4. First, the Remote Control operator requests the control for a specific HX using the remote control depicted by the sequence *Request Manual Control (HX_n)*. Next, the Fleet Control Server removes the requested HX_n from the autonomous operation (*Remove HX from Fleet*). Now the specific HX_n is informed that it is checked out from autonomous operation with the command *Check-out HX_n from fleet*. This would result in a state change within the specific HX. Additionally, the fleet control server provides a status for successful checkout of the HX by sending the status *Acknowledge Manual Control* to the remote control handheld. Once the remote control handheld receives this confirmation, the remote control operator can connect to the targeted HX depicted by the command *Connect Remote to HX_n*. The HX_n is approving the connection by sending *Approve Connection to Remote*. First after this has been successful, the Remote Control is getting the control over the targeted HX.

Concept 2 In Figure 5, a possible realization of concept 2 is depicted. In this case, the Remote Control directly communicates with the targeted HX, and the HX is checking itself out from the Fleet Control. The Remote Control is sending the request *Request Manual Control* to the targeted HX. Once the HX has received the request, the HX is sending the request *Request Checkout from FC* to be checked out from the fleet of autonomous vehicles to the Fleet Control. If successful, the Fleet Control is removing the HX from the autonomous fleet shown with the internal message *Remove HX from Fleet* to make the HX available for manual operation. Once approved, the Fleet Control is sending the approval *Approve Checkout of HX* to the requesting HX. The HX will then need to change state to enable the manual operation and send the approval for the manual operation to the Remote Control *Acknowledge Manual Control*. First after this has been successful, the Remote Control is getting the control over the targeted HX.

We did not add the Site Server and the Site Operator in the sequence diagrams shown above and limited the number of sequence to reduce the size of the diagrams for this paper.

In both concepts, there is a risk that the HX is checked out from the Fleet Control and not yet connected to the Remote Control, leaving it in an undefined state and, in the worst case, without connection to an emergency stop.

C. Step 3 - Create Table based on Sequence Diagrams

Once the interactions between the constituent systems are captured, these sequence diagrams shall support a hazard analysis. One challenge is how this information can be extracted to support the analysis. To show the conceptual applicability of

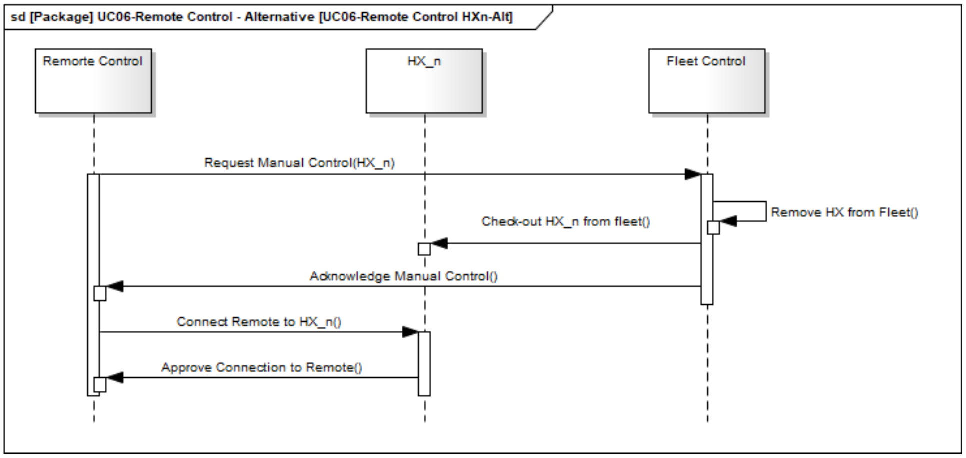

sd [Package] UC06-Remote Control - Alternative [UC06-Remote Control HXn-Alt]
Remorte Control
HX_n
Fleet Control
Request Manual Control(HX_n)
Remove HX from Fleet()
Check-out HX_n from fleet()
Acknowledge Manual Control()
Connect Remote to HX_n()
Approve Connection to Remote()

Fig. 4. Taking over HX for manual operation- Concept 1

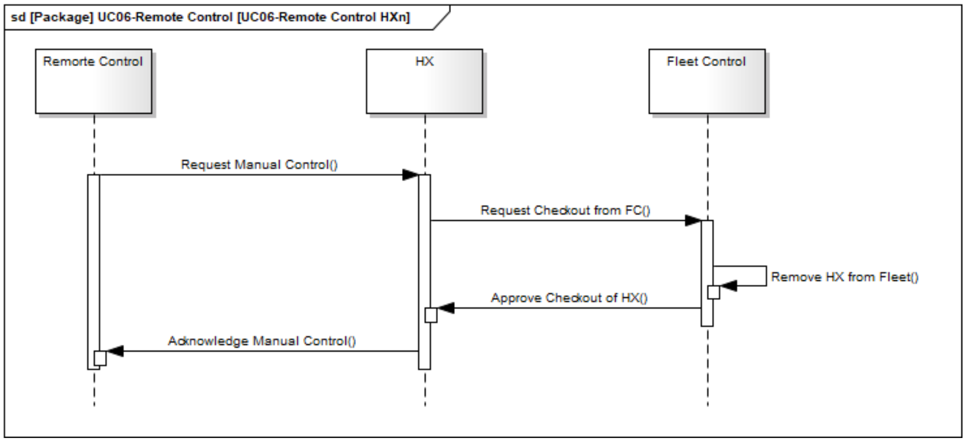

sd [Package] UC06-Remote Control [UC06-Remote Control HXn]
Remorte Control
HX
Fleet Control
Request Manual Control()
Request Checkout from FC()
Remove HX from Fleet()
Approve Checkout of HX()
Acknowledge Manual Control()

Fig. 5. Taking over HX using remote control - Concept 2

our approach, we utilized the xml export feature of the model-based development tool we use for modeling the sequence diagrams and transform this information to a table format which typically is applied for conducting a hazard analysis. In Figure 6 we show how the data is extracted from the sequence diagrams and prepared for analyzing the safety.

Once the behavior is documented in a sequence diagram (1), this diagram is exported to an XML file (2). We wrote a simple Python parser to transfer the information from the XML format to the table format needed (3) for further editing. Specifically, we extracted each message's source and target and the message name as an identifier. The source and target of each message provide the list of constituent systems, which are relevant for this specific analysis. Finally, the table is created (4) and can then be filled manually with the support of technical experts.

D. Step 4 - Hazard Analysis

During analysis of each concept, the table is filled in (5) as shown in the process in Figure 6. We are interested in the constituent systems and how a failure can contribute to possible accidents. Furthermore, the communication between the constituent systems is essential to be analyzed as well. The table created is therefore including both aspects. Specifically, we apply a hybrid between FMEA and HAZOP. In Figure 8 we present a simplified view of the table used for the hazard analysis created for concept1. The headers of each column are predefined, and the Python script from Step 3 is filling the list of constituent systems in column *Component* based on the sequence diagram. Then, depicting the communication channels, we use the prefix *Comm:*. Filling the table for the constituent systems (HX and Fleet Control in our case) is following the process from an FMEA with listing *Potential Failure Modes*, *Potential Causes of Failure* and *Potential Effects of Failure*. Then, for each potential effect of failure, the severity is estimated. In our case, the severity may range from 1 to 10, where 1 is least critical, and 10 correlates to an accident with several severe injuries. In Figure 8 we utilize severity 9 for risk for human safety and 6 for the stop of production. A failure in a system-of-system's context may differ between particular areas of operation. Therefore, we add the column *Geographic Area* to the table.

Suppose, due to a failure, a wrong HX is connected to the remote control. In that case, the unintended HX moving may be critical in the Remote Control Area, where humans potentially work or maintain machines. This may lead to critical accidents risking the safety of those humans (rows

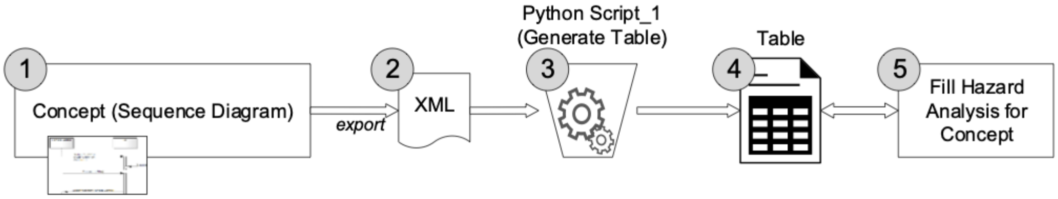
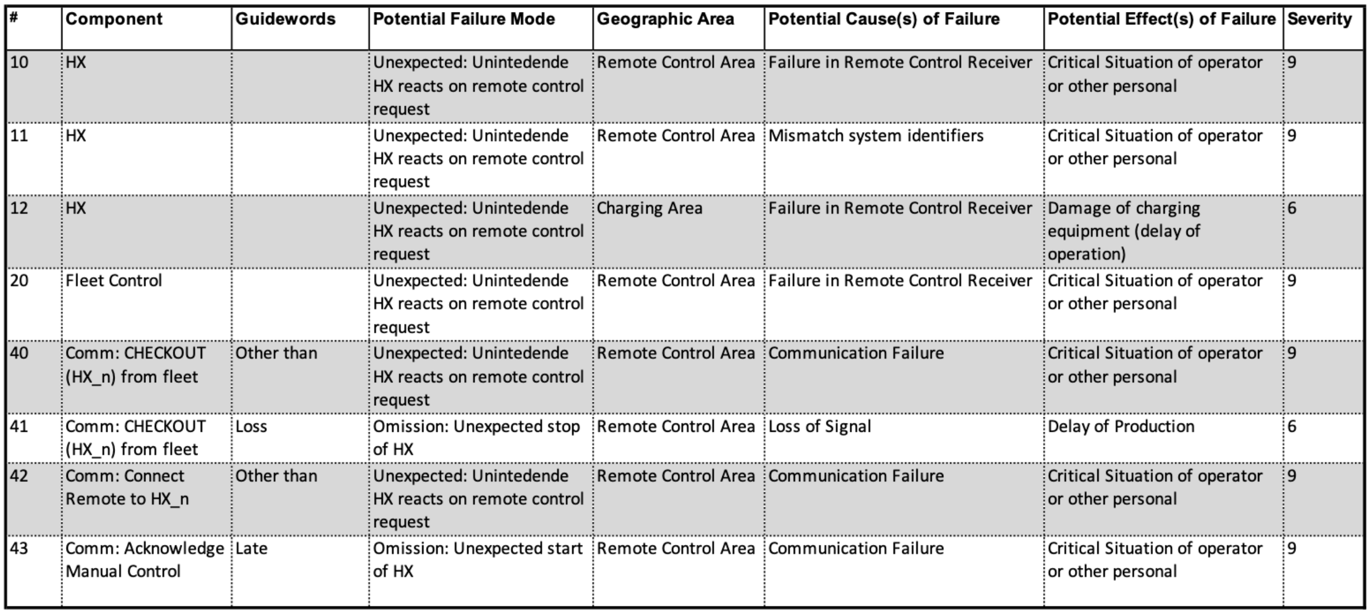


Fig. 6. Extracting information from Sequence Diagrams to support a hazard analysis



#	Component	Guidewords	Potential Failure Mode	Geographic Area	Potential Cause(s) of Failure	Potential Effect(s) of Failure	Severity
10	HX		Unexpected: Unintedende HX reacts on remote control request	Remote Control Area	Failure in Remote Control Receiver	Critical Situation of operator or other personal	9
11	HX		Unexpected: Unintedende HX reacts on remote control request	Remote Control Area	Mismatch system identifiers	Critical Situation of operator or other personal	9
12	HX		Unexpected: Unintedende HX reacts on remote control request	Charging Area	Failure in Remote Control Receiver	Damage of charging equipment (delay of operation)	6
20	Fleet Control		Unexpected: Unintedende HX reacts on remote control request	Remote Control Area	Failure in Remote Control Receiver	Critical Situation of operator or other personal	9
40	Comm: CHECKOUT (HX_n) from fleet	Other than	Unexpected: Unintedende HX reacts on remote control request	Remote Control Area	Communication Failure	Critical Situation of operator or other personal	9
41	Comm: CHECKOUT (HX_n) from fleet	Loss	Omission: Unexpected stop of HX	Remote Control Area	Loss of Signal	Delay of Production	6
42	Comm: Connect Remote to HX_n	Other than	Unexpected: Unintedende HX reacts on remote control request	Remote Control Area	Communication Failure	Critical Situation of operator or other personal	9
43	Comm: Acknowledge Manual Control	Late	Omission: Unexpected start of HX	Remote Control Area	Communication Failure	Critical Situation of operator or other personal	9

Fig. 7. Hazard Analysis for Concept1 (simplified)

10, 11, and 20). If an HX is located on the charger and unintendedly set to manual mode and start moving, it will damage the charging equipment (row 12). This will pause the production process until the charger is repaired.

For analyzing communication on this level, a Hazop is more suitable. A Hazop Analysis is utilizing guidewords to find hazards, and we add the column *Guidewords* to the table. In our example we apply the guidewords *Other than*, *Loss* and *Late* shown in Figure 8. The guidewords *Loss* and *Late* relate to the order and timing of a specific message. In comparison, the guideword *Other than* relates to the content of a message. In our case, the wrong ID of an HX in the message *Comm:Connect Remote to HX_n* in row 42 may lead to the situation that a wrong HX is connected to the remote control. The reason may be a bit-flip or interference of the communication channel if the final design is not adjusted.

For concept2, fewer messages need to be analyzed. Specific for concept2 is though that a failure in an HX could lead to unintended sending the message *Request Checkout from FC* to the Fleet Control. The HX will be disconnected from the autonomous operation and the remote control may be connected unintendedly.

The results from this analysis help to find suitable technical or process mitigations required by standards like ISO 12100 [8].

E. Step 5 - Transfer Results and enhance Sequence Diagrams

The results are parsed back to the original sequence diagram once the table is filled with failure modes and their effects. We again utilized XML as a file format and used a second Python script (6). The XML is imported to the sequence diagram, enhancing the diagram with information about the constituent systems and their commincation.

With this process's help, a sequence diagram can be used as a source for designing the system-of-systems.

F. Step 6 - Deriving of SoS Architecture

One limiting factor in deriving the concepts for specific SoS functionality is that the connection between operations and workflows is lost. Therefore, all decided concepts and their sequence diagrams can be combined to derive the system-of-system architecture displayed in Figure 9. Because of the rules we have set up when creating the sequence diagrams, all sequence diagrams on the SoS Meso Level contain the constituent systems and communication. This helps to map all constituent systems into a SysML component diagram. This process can also be automated. Since the sequence diagrams are enhanced with information from the hazard analysis, this information is transferred to the component model.

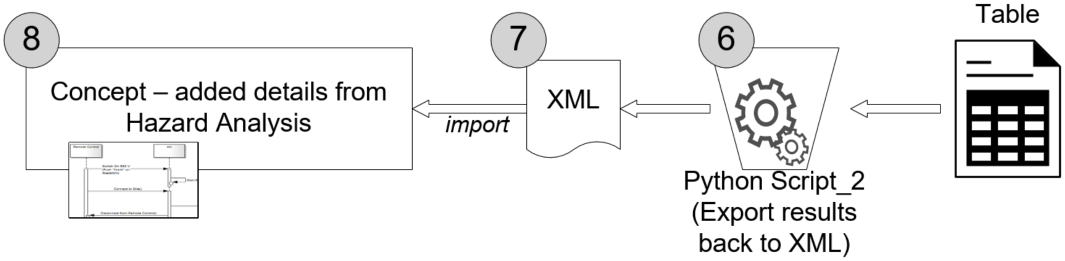


Fig. 8. Feeding the information back to the sequence diagram

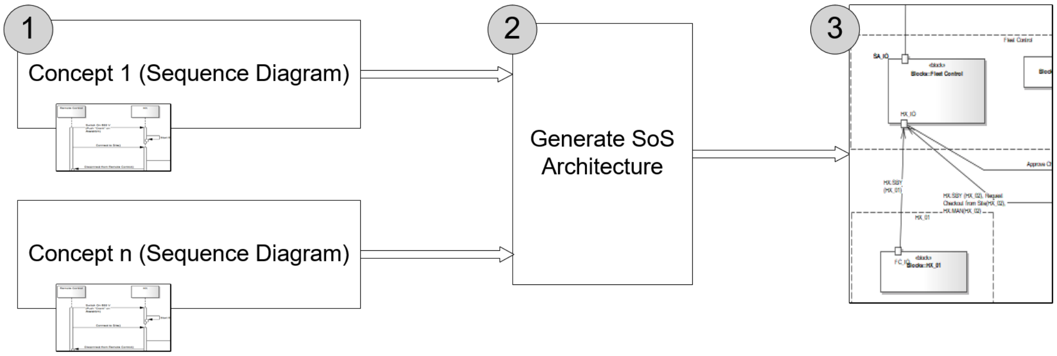


Fig. 9. Creating system-of-systems architecture based on chosen concepts

V. Analysis

A. Structure Base for Analysis

Compared to the documentation of behavior in text, the sequence diagrams provide a structured data source for the analysis. However, the vast complexity of a system-of-systems would require high efforts for analyzing the safety. By focusing on single concepts, the scope is limited and easier to handle.

B. Identification of Emergent Hazards

When analyzing the concepts of a system-of-system function, the following emergent hazard types can be identified:

Interface Hazards Hazards related to the interfaces imply that failures are transmitted through the interfaces, leading to an accident in a different constituent system. Our approach enables the identification of interface hazards for the constituent systems involved in sequence diagrams. Thus, the possibility of finding failures cascading through a net of systems is limited to the constituent systems included in a sequence diagram.

Resource Hazards The constituent systems share resources, such as the wireless network. Therefore, when analyzing the messages in our method, we can find and analyze those messages requiring higher reliability. This information can then be used during the design process to ensure reduced proneness for errors due to flaws in communication.

Interoperability Hazards Interoperability hazards relate to how constituent systems interpret a received message. For example, different applied data formats may lead to misinterpreting received data and potential accidents. In our hazard analysis, we can find some scenarios where data is misinterpreted. This is limited to the constituent systems involved in a sequence diagram.

C. Limitations

a) Additional information required: Utilizing sequence diagrams for documenting the interaction between constituent systems is not sufficient. We pointed out above that we expect, for example, that an HX is changing the state from autonomous mode to manual mode during the take-over control scenario. However, this information is not available in the sequence diagrams. Therefore, capturing the state machines of the constituent systems is necessary. For this purpose, we have tried Petri Nets in our previous work [25].

b) Limitation to find cascading failures: The constituent systems are communicating, and a communicated faulty message may lead to an accident of a constituent system after this message has been cascading through the network. One challenge with the hazard analysis approach we apply in our context is that a cascading failure through a network of constituent systems is hard to identify.

VI. Conclusion and Future Work

This paper presents a case from the earth-moving machinery domain, where autonomous machines are used in an open surface mining context. These autonomous vehicles are operated in a fleet and are integrated into existing production processes, including other human-operated vehicles and machines. Such a system can be seen as a system-of-systems with complex interactions between the involved constituent systems. There is a lack of clear processes and methods to engineer such system-of-systems to support, among others, the safety standard compliance. The main focus of this paper is how to evaluate concepts when designing a system-of-systems. We propose a structured process including deriving the general concepts and documenting those concepts using sequence diagrams. The sequence diagrams capture the interaction between the constituent systems in a system-of-systems. This data is then transferred into a table format to conduct a hazard analysis. For analyzing hazards, we utilize a hybrid between FMEA and HAZOP to identify both potential failures of the constituent systems and risks related to communication among them. Specifically, we can to a certain extent identify the emergent hazard types: interface, interoperability, and resource hazards. The results from this analysis are fed back into the sequence diagrams. Additionally, we provide an outlook towards how the sequence diagrams can help to derive the system-of-system architecture.

Further research is necessary to trace the findings from the hazard analysis through each development stage when designing a system-of-systems.

Acknowledgement

The authors acknowledge the funding support received for this research from the KKS-funded ITS-EASY Post Graduate School for Embedded Software and Systems, FiC Project (SSF) and ESCAPE Project (Vinnova).

References

[1] CMMI Product Team, “CMMI for Development, Version 1.3,” Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2010-TR-033, 2010. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9661

[2] International Organization for Standardization, “ISO/IEC (2015) ISO/IEC 33001:2015 Information technology – Process assessment,” 2015.

[3] ——, “ISO 26262:2018 - Road vehicles Functional safety,” 2018.

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

[5] C. Ericson, *Hazard analysis techniques for system safety*. Wileys, 2016.

[6] 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.

[7] ——, “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/

[8] International Organization for Standardization, “ISO 12100 Safety of machinery - General principles for design - Risk assessment and risk reduction,” 2010.

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

[10] International Electronical Commission, “IEC 61025 - Fault Tree Analysis (FTA),” 2006.

[11] United States Department of Defense, *MIL-STD 1629A - Procedures for Performing a Failure Mode, Effect and Criticality Analysis*, 1980. [Online]. Available: http://www.fmea-fmeca.com/milstd1629.pdf

[12] International Electronical Commission, “IEC60812:2018 Failure modes and effects analysis (FMEA and FMECA),” 2018.

[13] ——, “IEC 61882:2001 Hazard and operability studies (HAZOP studies) Application guide,” 2001.

[14] D. Macdonald, *Practical Hazops, Trips and Alarms*, D. Macdonald and S. Mackay, Eds. Oxford: Newnes, 2004.

[15] P. J. Redmond, “A System of Systems Interface Hazard Analysis Technique,” 2007. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a467343.pdf

[16] United States Department of Defense, “MIL-STD-882E,” Washington, DC, USA, 2012.

[17] International Organization for Standardization, “ISO/IEC/IEEE 21841 Systems and software engineering Taxonomy of systems of systems,” 2019.

[18] M. Mori, A. Ceccarelli, P. Lollini, B. Frömel, F. Brancati, and A. Bondavalli, “Systems-of-systems modeling using a comprehensive viewpoint-based SysML profile,” *Journal of Software: Evolution and Process*, vol. 30, no. 3, pp. 1–20, 2018.

[19] J. Guiochet, G. Motet, C. Baron, and G. Boy, “Toward a Human-Centered UML For Risk Analysis - Application to a medical robot,” in *Human Error, Safety and Systems Development*, 2004.

[20] 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.

[21] J. El Hachem, Z. Y. Pang, V. Chiprianov, A. Babar, and P. Aniorte, “Model Driven Software Security Architecture of Systems-of-Systems,” in *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, 2016, pp. 89–96. [Online]. Available: https://ieeexplore.ieee.org/document/7890575/

[22] 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/

[23] S. Baumgart, J. Fröberg, and S. Punnekkat, “Defining a Method to Perform Effective Hazard Analysis for a Directed SoS Based on STPA,” in *Third Swedish Workshop on the Engineering of Systems-of-Systems 2018*, 11 2018. [Online]. Available: http://www.es.mdh.se/publications/5599-

[24] ——, “A Process to Support Safety Analysis for a System-of-Systems,” in *The 31st International Symposium on Software Reliability Engineering (ISSRE)*, 2020.

[25] ——, “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-