Defining a Method to Perform Effective Hazard Analysis for a Directed SoS Based on STPA

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

***Abstract*—Automating a quarry site as developed within the electric site research project at Volvo Construction Equipment is an example of a directed system-of-systems (SoS). In our case automated machines and connected smart systems are utilized to improve the work-flow at the site. We currently work on conducting hazard and safety analyses on the SoS level. Performing a hazard analysis on a SoS has been a challenge in terms of complexity and work effort. We elaborate on the suitability of methods, discuss requirements on a feasible method, and propose a tailoring of the STPA method to leverage complexity.**

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

I. Safety analysis for SoS

We are currently working with safety analysis of an intended automated quarry, and the objective of this paper is to present our approach with using STPA and elaborate on how to define an effective method to perform hazard analysis in a system-of-systems (SoS).

Safety and hazard analysis methods such as Preliminary Hazard Analysis (PHA), Failure-Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) [1] are well established in industry and these methods are required by functional safety standards. Today's industrial development processes are often tailored to develop single systems, where the intended operational context is used as an important input when analyzing potential hazards. As single systems get more automated and connected to its surrounding world, their behavior becomes more advanced. They become smarter in the sense that they exhibit more functionality and thus safety analysis takes a larger effort.

When products are connected to form a SoS, their ability to interact and share services and signals to achieve cooperative goals need to be explicitly addressed. The usage may deviate from what was intended for a single product. Interactions and emergent behavior in a SoS can give rise to hazards and unsafe work environment although each system in itself is already analyzed thoroughly. The application of standard hazard and safety analysis methods for analyzing a SoS may not be enough and it may not be the most efficient method.

II. Industrial Case - An Automated Quarry

The automated quarry site in our case is operated with machines and other systems that are cooperating to meet goals of productivity and quality, but also a safe and hazard-free work environment. Many of the constituent machines are highly automated and are connected to off-board systems to monitoring of the production process. In our case, the quarry is a surface mine with different production stages, where material is transported by haulers between production steps for further processing. In the electric site research project [2], the work-flow at the site is adapted by using automated haulers, called HX, for material transporting purposes. The HX machines operate in a fleet and are track-based automated guided vehicles (AGVs) (Fig. 1) [3], which receive their work-missions from a fleet control system. Knowing the correct position of all involved machines is necessary for executing missions and avoiding accidents.

An excavator loads a crusher that loads crushed rocks directly onto semi-automated haulers that, in turn, transport and tip the material to a secondary crusher. The operation is supported by several information systems. A site management system is operated by a site operator to monitor production and tune the production process. Machines are also connected to maintenance and fleet management systems. Some machines are equipped with positioning systems.

The site system is an example of a system-of-systems where different smart systems are independent in terms of management, ownership and life-cycle. This is a directed SoS [4] and the constituent systems use their abilities to cooperate to achieve production in the quarry. Furthermore, the constituent systems use smartness to optimize, e.g., machine wear or energy consumption, giving rise to emergent behaviors. But some emergent behavior could be unwanted or even associated with risk. Constituent systems are typically part of more than one SoS, and the involvement can vary over time, e.g., machines are added, removed or updated with new features.

A typical hazardous scenario could be that constituent systems may change state due to internal reasons and possibly assume a change in operation that another constituent system do not. Providing a machine position, for example, may not

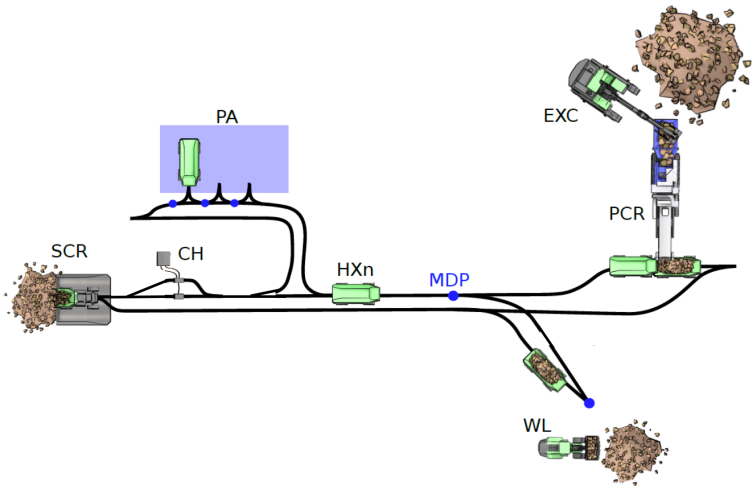

Fig. 1. An automated Quarry

be considered when the machine is in repair mode. Another typical critical scenario could be that a certain system relies on the correctness of information that is shared by another. A critical situation can occur, if signals are provided incorrectly, or interpreted differently by the receiver. Such hazards would not show up when analyzing hazards of the single system by itself.

III. Hazard Analysis Methods

There are mature hazard and safety analysis methods in literature, which are applied in industry today. Among the most well-known methods are Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA) and Hazard and Operability Analysis (HAZOP). FTA is a top-down technique where each possible unwanted state is investigated based on which combinations of events could lead up to it. FMEA is a bottom-up approach where foreseeable faults of components of a system are analyzed with respect to likelihood and negative effects. Hazard and Operability analysis (Hazop), has its roots in the chemical industry and is utilizing guide words for identifying hazards and critical scenarios with respect to operations.

We have especially looked at the systems theoretic process analysis (STPA) [5], which is a method to model accident causation.

IV. Requirements on a low-footprint hazard analysis method

In our work we have so far applied FMEA and STPA, but run into problems with completing due to complexity and unfeasible work effort. Thus we strive for a method with lower footprint that would still aid in analyzing the potentially hazardous interactions within our quarry. We aim to tailor a method that provides:

- Abstraction of each system detail just the interaction and collaboration between constituents in the SoS should be analyzed. This includes state changes such as start-up, and maintenance breaks, but not internal handling of them.
- Reasonable footprint - the system must be described in such a way that complexity is manageable from a work effort perspective.
- Effective in finding hazards. In order to be meaningful, the method should find hazards that are not apparent at a first glance.

V. Analysis

The STPA method includes defining a controls structure that encompass which entities control which and what control signals that are involved. After the control structure is defined, the method is used to find possible loss scenarios. When we applied the STPA method, we saw a number of areas that presented challenges to us:

- The complexity of the system on the quarry did lead to high efforts for conducting STPA. Using all the items in the system blueprints that were given to us by engineers lead to an overly complicated control structure.
- It is important to describe or model the usage of a SoS. Not only the technical structure. There are control signals that are not shown in a technical schematic, e.g., a wave of hand by a manager.
- Analyzing many interacting smart products can cause a state explosion.
- Non-persistent analysis because products receive functional updates and thereby change behavior. There are rarely defined limits as of how much a product behavior can change when its software is updated.
- Hazards can be caused by simultaneous changes in control signals. We see that such hazards are difficult to identify in complex SoS.

VI. Proposed tailored method of STPA

One major finding from applying STPA in our case is that it is difficult to find the right level of detail for a control structure. Too much detail leads to a situation with too many signals (control actions) which in turn lead to high effort for performing the analysis. A second finding is that it is very easy to focus too much on system internals when analyzing the loss scenarios. Instead, we propose to focus on only the interaction between systems in the SoS, in order to avoid getting stuck in details of a specific system. In order to come up with a light weight method, we have devised three principles to aid us in getting a handle on the high complexity of the system.

- As a first step in the "Define purpose" phase of STPA, we define only the constituent systems. No internals or internal control actions are revealed. We define the control structure based on this simplified model. This means that each constituent system can never be modelled with more than one box in the control diagram.
- We add a step where we define system usage for each constituent in the form of use case descriptions. Based on the use cases, we elicit all signals that are involved, and we perform the "unsafe control actions" analysis based on these signals. The STPA does not explicitly address use case description, and we advocate it as an intermediate step to aid in getting the control diagram right. By using the use-case descriptions we see a way to focus on only the signals that matter rather than going through all signals that exist between systems.
- We perform an extra step of checking the signals for simultaneous changes that could cause hazards.

VII. Application in Case

By applying our method we got the control structure diagram described in Fig 2.

We go through the usage for each actor and define use cases. Based on our use cases we filter out each safety critical control signal and use that as an input to analysis of unsafe control actions. When the signals are listed in a table, we also check for problems caused by simultaneous changes. We did see indications of potential problems in scenarios when two different actors try to simultaneously change state of the same system.

VIII. Conclusion

Performing a hazard analysis is an important task when designing a complex directed SoS and many safety methods are aimed at single systems. We have applied STPA in an industrial case of a quarry and elaborated on our approach. When faced with the drawings and complex description of an industrial system there is a need to simplify and leverage the analysis procedure. We have come up with three principles to tailor the STPA procedure. We present the case and an example of the simplified control model.

References

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

[2] Volvo Construction Equipment, "Electric Site Project." [Online]. Available: https://www.volvoce.com/global/en/news-and-events/news-and-press-releases/2017/conexpo-vegas-2017/volvo-ce-unveils-the-next-generation-of-its-electric-load-carrier-concept/

[3] A. Jafari, J. J. S. Nair, S. Baumgart, and M. Sirjani, "Safe and Efficient Fleet Operation for Autonomous Machines: An Actor-based Approach," in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, ser. SAC '18, 2018.

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

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

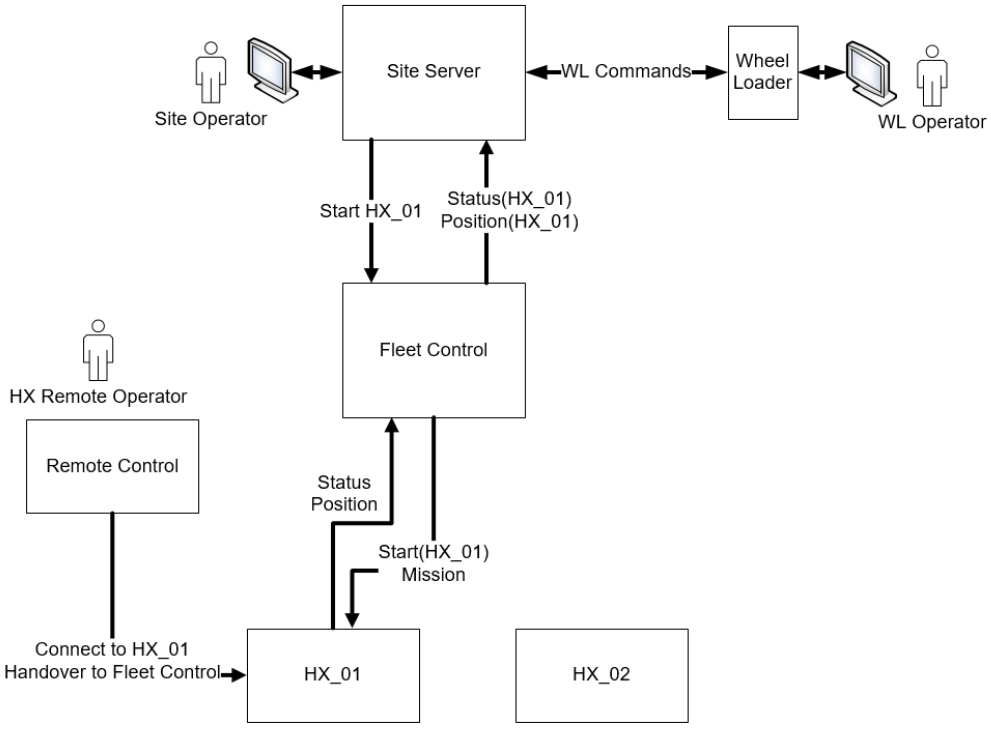

Fig. 2. Control Structure Diagram for STPA to study concepts.