2.4 Controlling interactions with other systems

Assurance objective - Identify how interactions between the RAS and other systems may give rise to unsafe behaviour.

Practical guidance – cross-domain

Authors: Muhammad Atif Javed, Faiz Ul Muram, and Sasikumar Punnekkat (Mälardalen University, Sweden)

Overview of approach

A structured process is required to document a system-of-systems in a structured way – we call this concept SafeSoS, indicating that the purpose is to enable a safety analysis and identifying critical situations.

We apply the hierarchical levels described by Axelsson[4] 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 are analysed. This information is refined in the meso analysis, where information on how the constituent systems form is analysed. 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 1 the SafeSoS process is shown with descriptions on the macro level, meso level, and micro level. For each of these levels, we distinguish between information with respect to structure and behaviour 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.

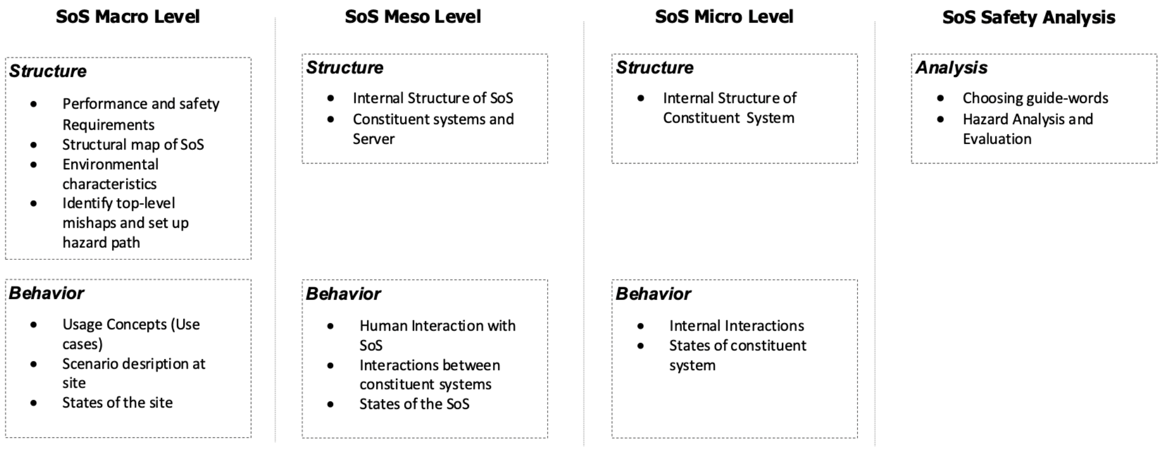
SoS Macro Level
Structure
Performance and safety Requirements
Structural map of SoS
Environmental characteristics
Identify top-level mishaps and set up hazard path
Behavior
Usage Concepts (Use cases)
Scenario desription at site
States of the site
SoS Meso Level
Structure
Internal Structure of SoS
Constituent systems and Server
Behavior
Human Interaction with SoS
Interactions between constituent systems
States of the SoS
SoS Micro Level
Structure
Internal Structure of Constituent System
Behavior
Internal Interactions
States of constituent system
SoS Safety Analysis
Analysis
Choosing guide-words
Hazard Analysis and Evaluation

Figure 1 - SafeSoS Process Steps

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.

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 of losses based on criticality. Based on the provided information, it can be analysed 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.

Meso level

In the SoS Meso Level, the internal perspective of the SoS with a focus both on the internal structure and interactions between the constituent systems are captured. System Designers and safety engineers can provide the required information.

Micro level

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

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

Safety analysis

As a safety analysis, HAZOP [5] was applied. This method is utilizing guide words to support the analysis team in identifying critical situations.

Typical examples of guidewords are:

- NO or NOT: Indicating an 'Omission fault' like not providing required messages or human error, if an expected action is not provided. This depends on the abstraction level looked at.
- MORE: similar to Commission fault. MORE can characterize environmental changes or MORE speed of a specific constituent system. Reconfiguration may be reflected by this guideword when for example the number of constituent systems is changing.
- LATE: similar to a 'timing fault'. Delayed identification of unauthorized personal or delayed communication of actual position of machinery, may result in critical situations. The causes differ again based on the abstraction level
- INCORRECT: similar to a 'value fault', is covering those faults related to the exchange of complex messages between constituent systems.

Industrial case study - electric site

The electric site research project [1] as a use case was used as a use case for applying this guidance. In this project, a fleet of automated guided vehicles (AGVs) called HX or TA15 are used to transport material at a quarry site, which is a surface mine for gravel production. The pre-crushed material is transported from a movable primary crusher to a stationary secondary crusher. Along with the fleet of autonomous HXs, a human-operated wheel loader and a human-operated excavator are used for loading material onto the HX. In our earlier works, we have described and analysed this complex SoS [2][3].

The fleet of active HXs is controlled by the Fleet Control System, containing features like traffic management or setting missions for each active HX. Each HX is therefore highly dependent on the wireless network and correct commands being received from the control system. It is furthermore possible to manoeuvre a single HX using a handheld remote control. Remote control using the handheld unit is limited to a single HX at once. This is typically used to activate an HX in the morning, remove an HX for repair, or adding an HX to a running production. The Site Operator is monitoring the quarry site from a control room, where the Site Server is located. In Figure 2 the involved systems and human operators in the context of remote take over are presented. When designing such a system an in-depth analysis of this scenario is necessary to identify potential hazards leading to critical accidents.

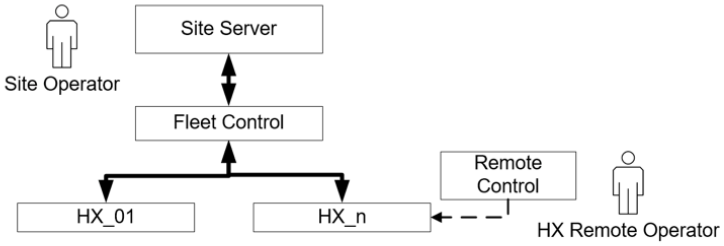

Figure 2 - Use Case: Remote Control of HX

References

- [1] Volvo Construction Equipment, "Electric Site Project." [Online]. 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/
- [2] S. Baumgart, J. Froberg, and S. Punnekkat, Analyzing hazards in system-of-systems: Described in a quarry site automation context, Annual IEEE International Systems Conference (SysCon), 2017, [Online]. http://ieeexplore.ieee.org/document/7934783/
- [3] S. Baumgart, J. Froberg, and S. Punnekkat, Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site, IEEE International Systems Engineering Symposium (ISSE), no. 4, 2018, [Online]. https://ieeexplore.ieee.org/document/8544433/
- [4] Jakob Axelsson, A Refined Terminology on System-of-Systems Substructure and Constituent System States, In Proceedings of the 14th Annual Conference System of Systems Engineering (SoSE), 2019
- [5] IEC 61882:2001, Hazard and operability studies (HAZOP studies) — Application guide
- [6] Stephan Baumgart, Joakim Fröberg, Sasikumar Punnekkat. A Process to Support Safety Analysis for a System-of-Systems, In Proceedings of the 31st International Symposium on Software Reliability Engineering (ISSRE 2020), October 2020