HAZARD ANALYSIS OF A FLEET OF AUTONOMOUS MACHINE USING STPA - A CASE STUDY

Stephan Baumgart, Volvo Construction Equipment

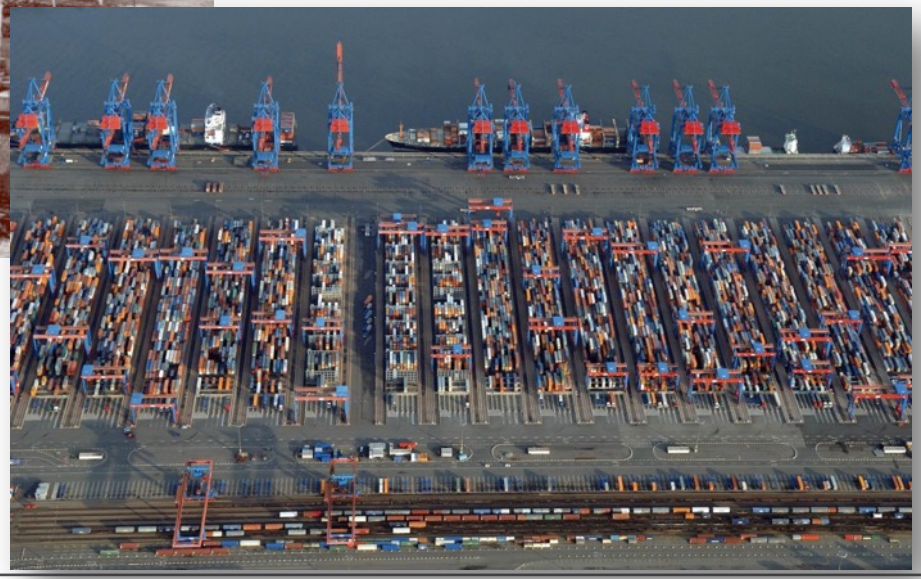
Scandinavian Conference on SYSTEM & SOFTWARE SAFETY 2019-10-23

Agenda

1. Introduction
2. Use Case Automated Quarry Site
3. Hazard Analysis Methods
4. STPA Introduction and Application
5. Insights
6. Future Directions

1. Introduction

Harbor / Container Terminal

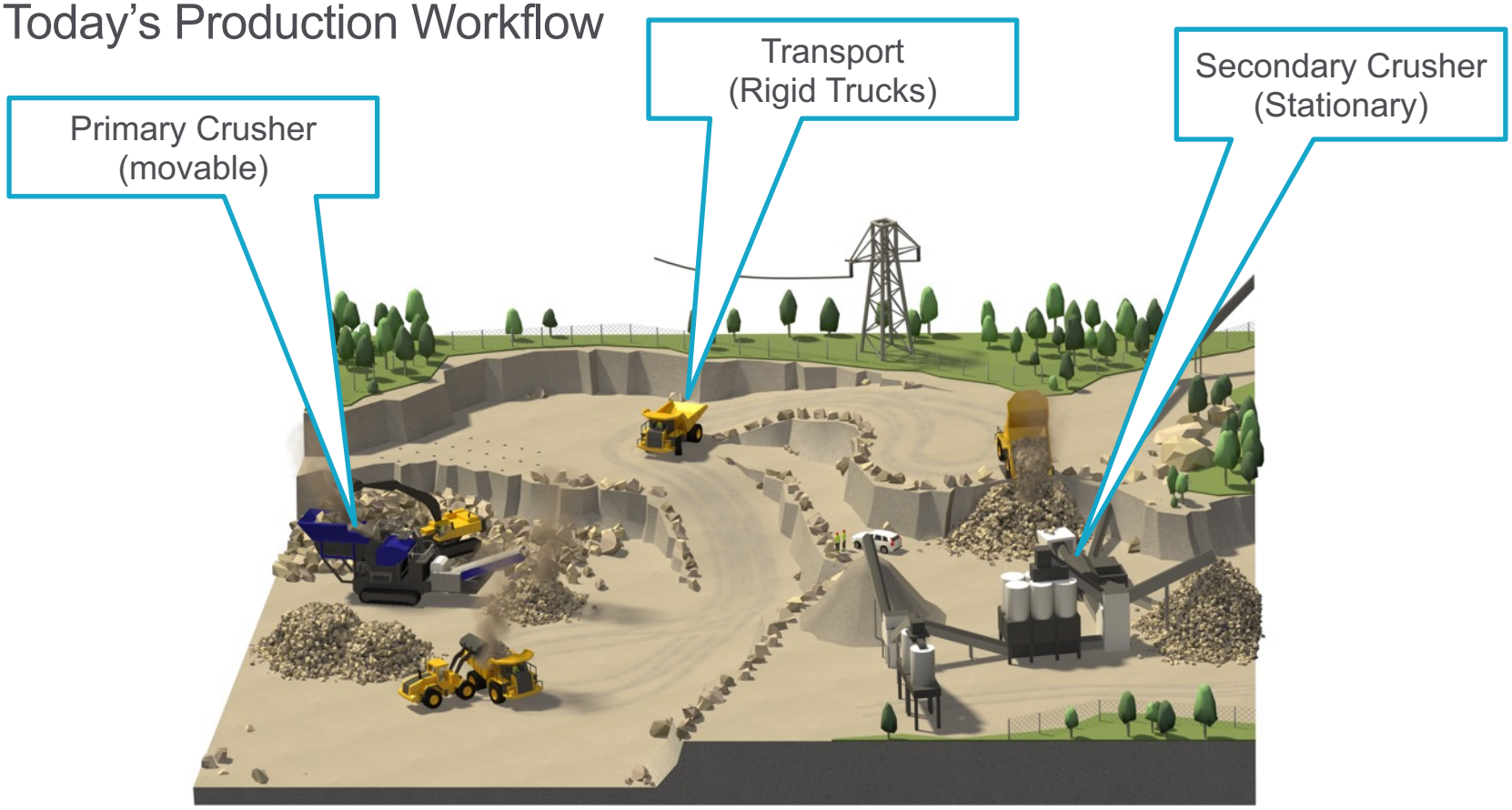


1. Introduction

Quarry / Quarry

Use Case: Automated Quarry Site

Today's Production Workflow



Research Initiative 1

Automated Quarry Site

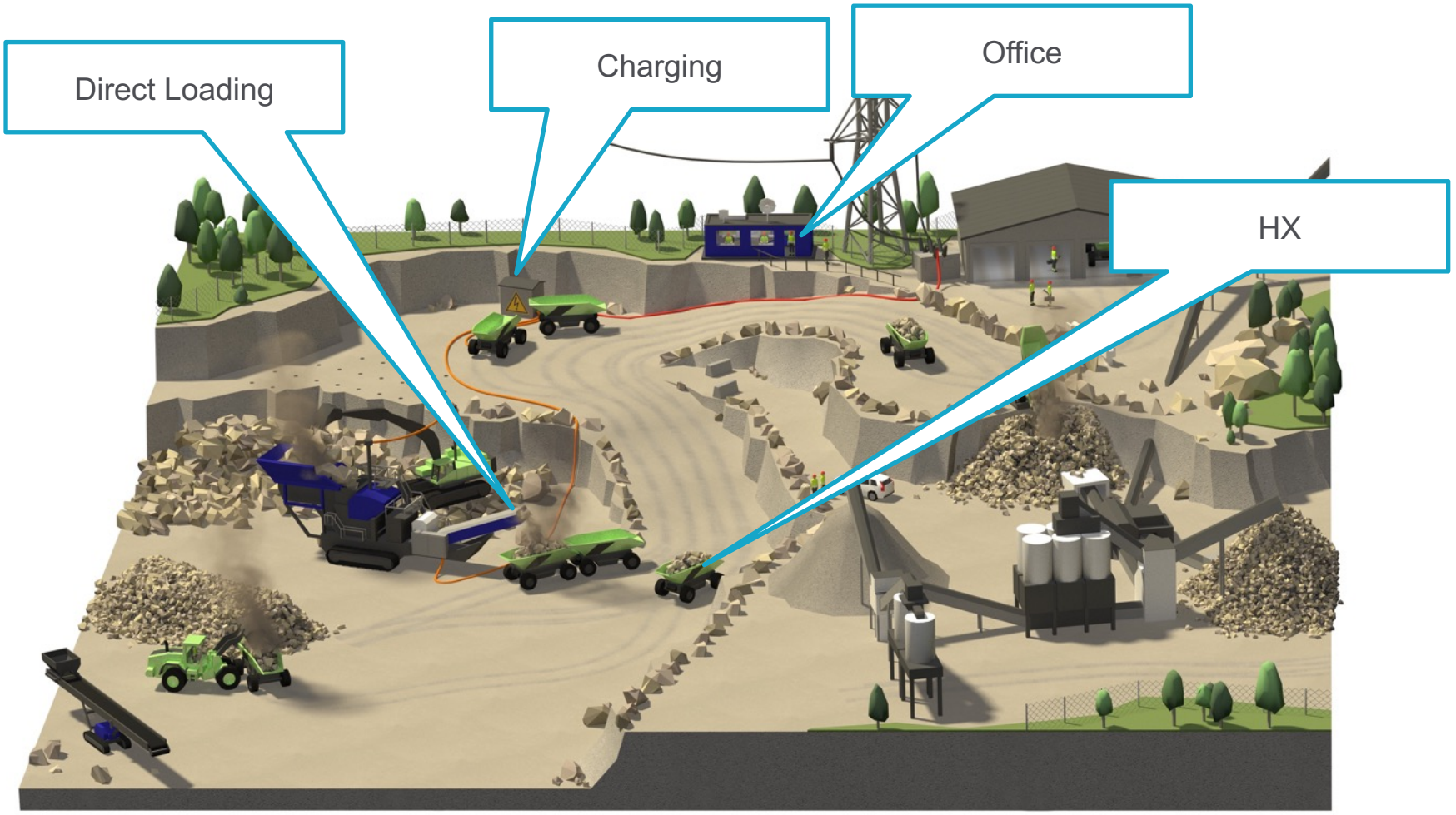
- Electric Site Research Project: collaboration between Volvo CE and Skanska and funded by the Swedish Energy Agency
- Project Goals:
  - ❖ Reducing CO2
  - ❖ Automating parts of the production
- Project Test Ground: Skanska Quarry Site
- Demonstration: Q4 2018

SKANSKA

Swedish Energy Agency

Use Case: Automated Quarry Site

Targeted Workflow

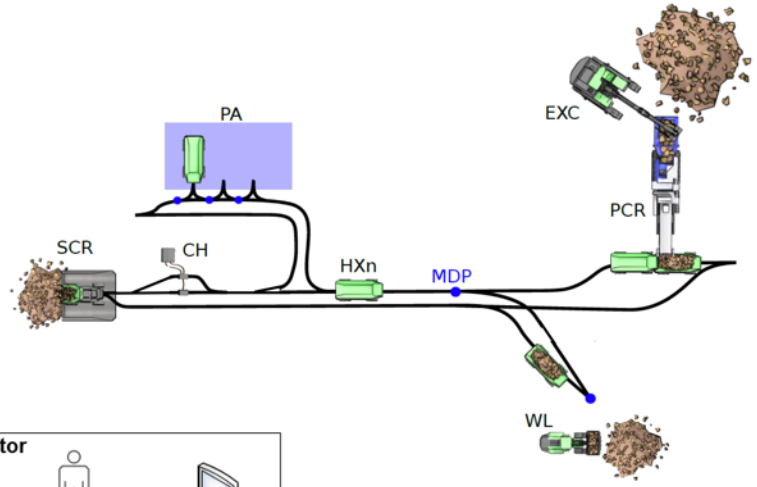


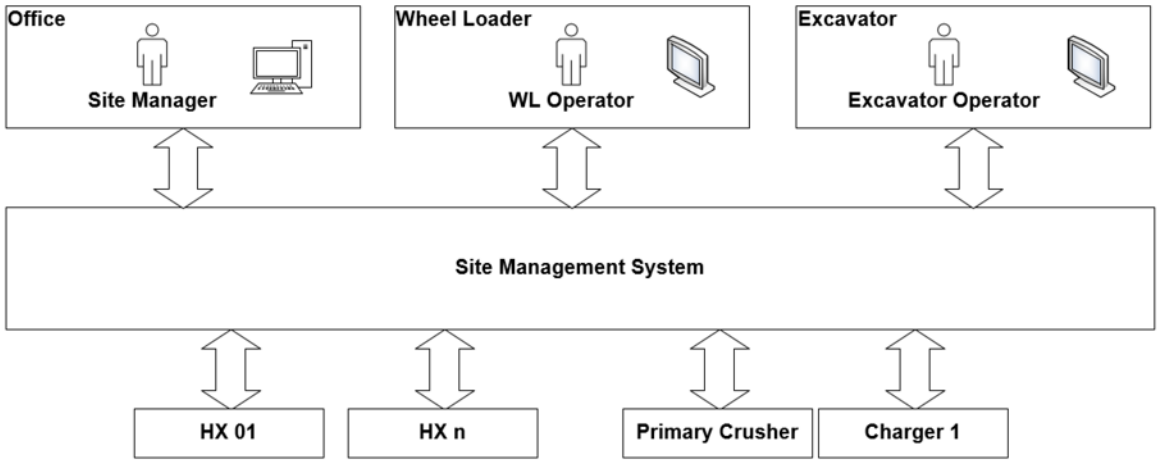
Use Case: Automated Quarry Site

Use Case: Automated Quarry Site

Routing

- Directed System-of-Systems
- HX = AGVs (Automated Guided Vehicles)
- Track-based





Research Initiative 2

Safety & System-of-Systems

- SUCCESS project
  (Safety Assurance of Cooperating Construction Equipment in Semi-Automated Sites)
- Focus on Safety for System-of-Systems

UNIVERSITY of York

MÄLARDALEN UNIVERSITY SWEDEN

ASSURING AUTONOMY INTERNATIONAL PROGRAMME

What are the Challenges?

- Focus on Safety (Avoiding Accidents)
  - How to achieve safety in a system-of-systems?
  - How to identify hazards on system-of-systems level?
    - Cascading through Network
    - Interaction between involved systems

Safety Analysis in General

Today's concepts:

- Focus: Single Human-Operated Machines
- Analysis Methods: PHA, FMEA, FTA
- Standard Support IEC 61508, ISO 13849, ISO 26262, …

➢Functional Safety

What is different?

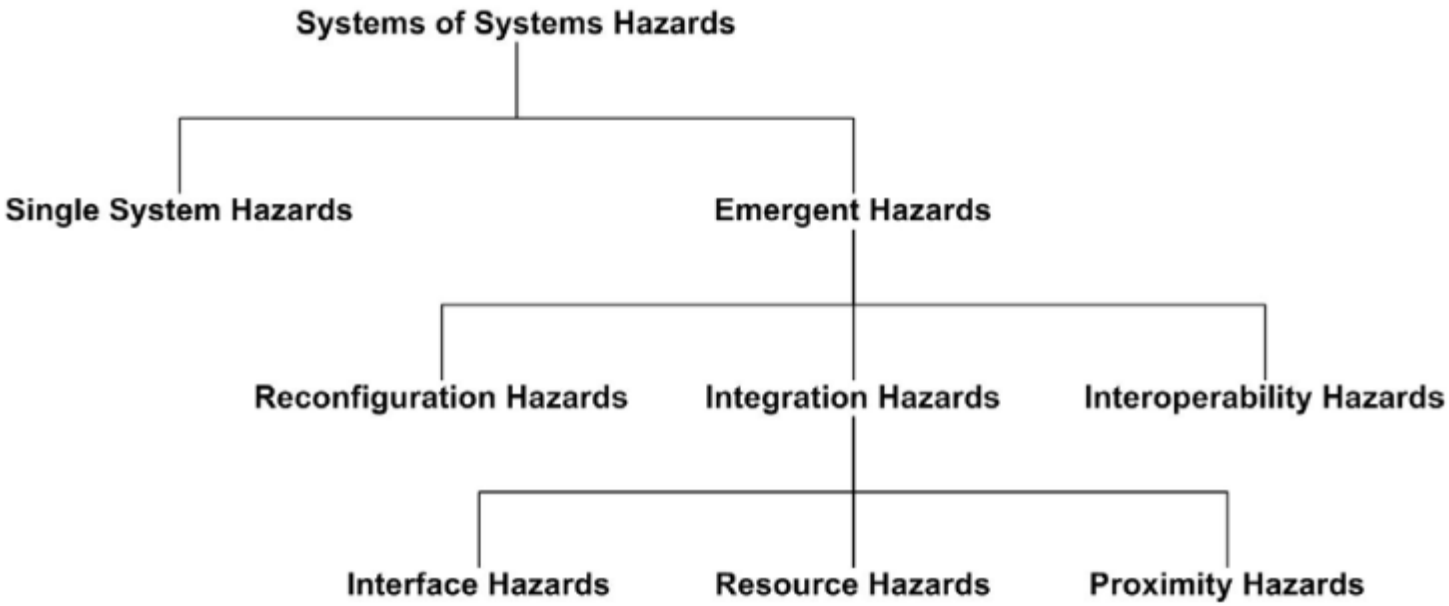
- Hazard Definition (ISO 26262:2018): potential source of *harm* caused by *malfunctioning behavior* of the *item.*

➢ Hazardous behavior not only caused by malfunction?

- Hazard Definition (STPA): A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.

Safety Analysis in General

Types of SoS Hazards



Redmond et al., ” Interface Hazard Analysis for System of Systems”, SOSE 2008

Safety Analysis in General

Today's concepts:

- Focus: Single Human-Operated Machines
- Analysis Methods: PHA, FMEA, FTA
- Standard Support IEC 61508, ISO 13849, ISO 26262, …

System-of-Systems Hazard Analysis

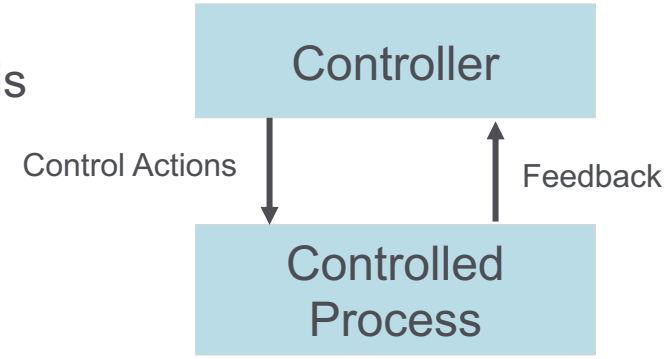
- SoSHA (System-of-System Hazard Analysis)
- Interface Hazard Analysis
- STPA (System-Theoretic Hazard Analysis)

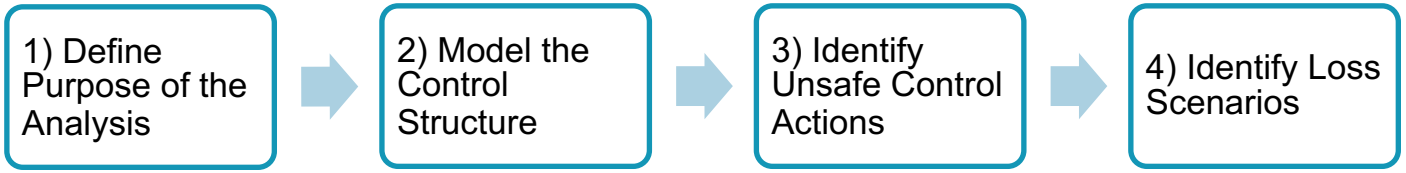
➢Standard Support? ISO 21448:2019 – SOTIF?

Integrating Existing Systems into a SoS
Example: Military Scenarios

What is STPA?

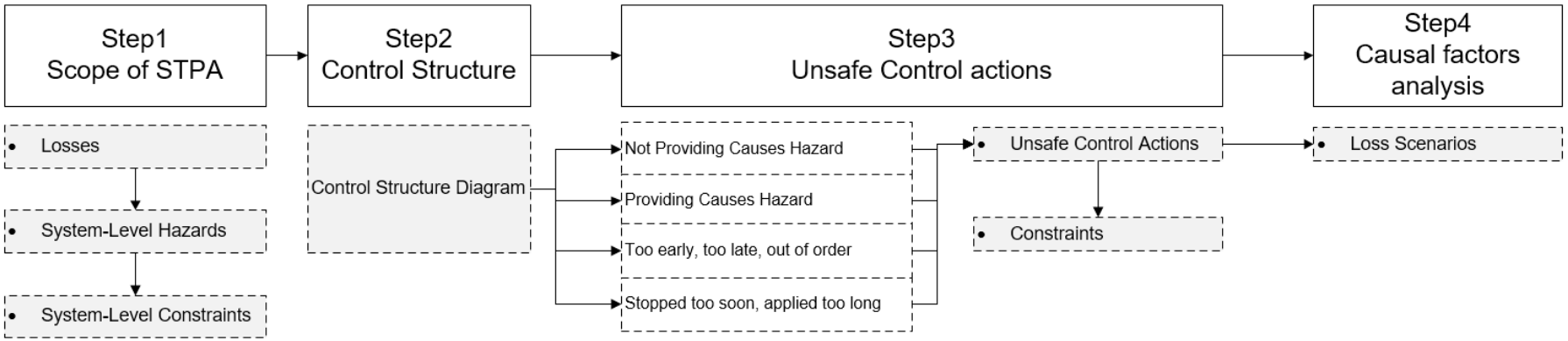
- Based on STAMP (System-Theoretic Accident Model and Processes) (Leveson)
- STPA – System Theoretic Process Analysis
- New Hazard Analysis Technique





STPA Handbook (Leveson, Thomas)

STPA -Process



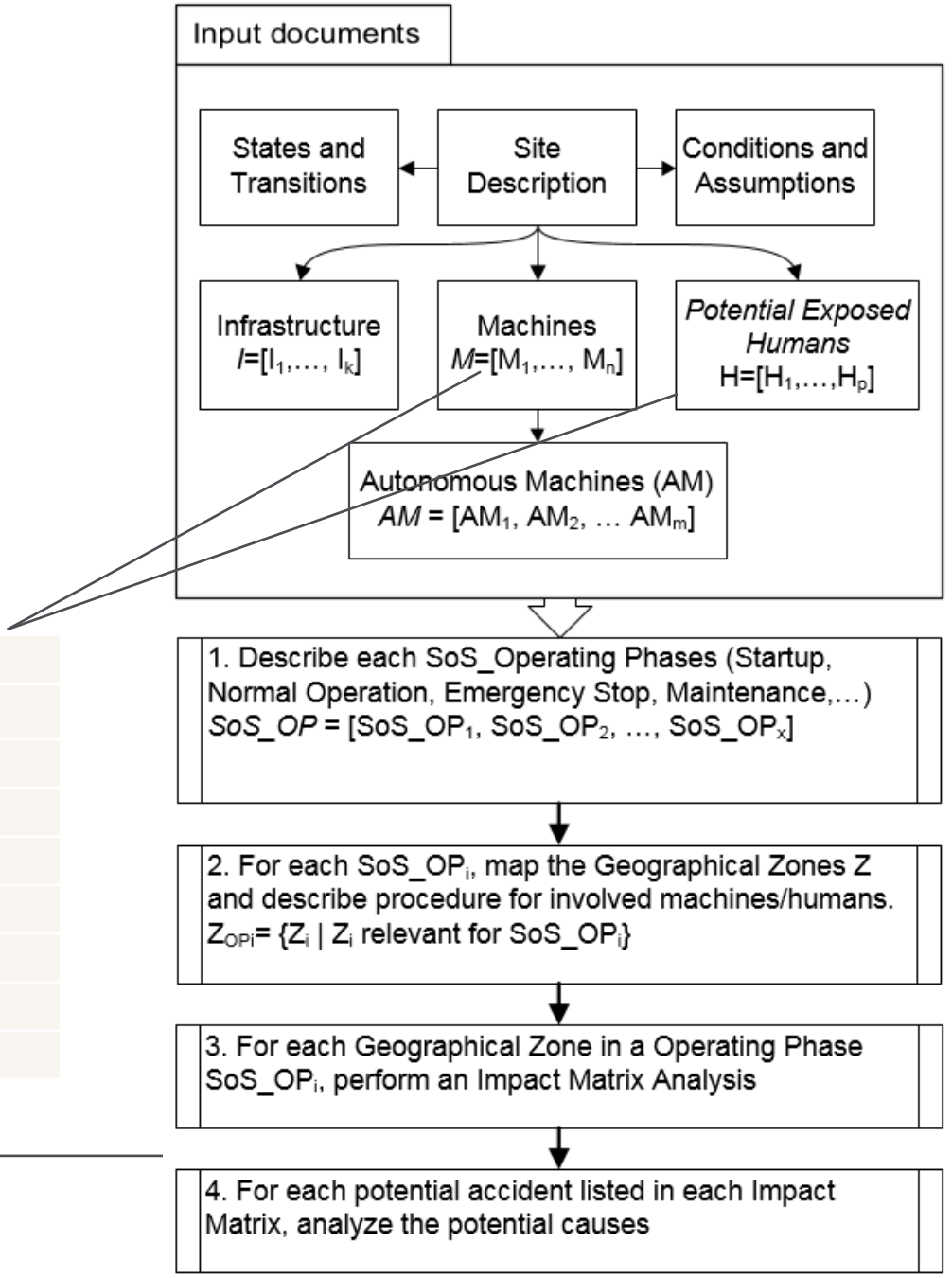
Insights

- Easy to get started
- Target:
  - System with high degree of details
  - Support developers
  - Research Project:
    - Agile development = architecture changed -> impact on Control Structure Diagram
- Control Structure Diagram:
  - Finding good abstraction level is a challenge
  - Necessary to add all involved systems? Simplification – only 2 HX
  - Knowledge about the Site and targeted processes/use case is necessary
  - Meetings: Several workshops with developers and experts required

Insights

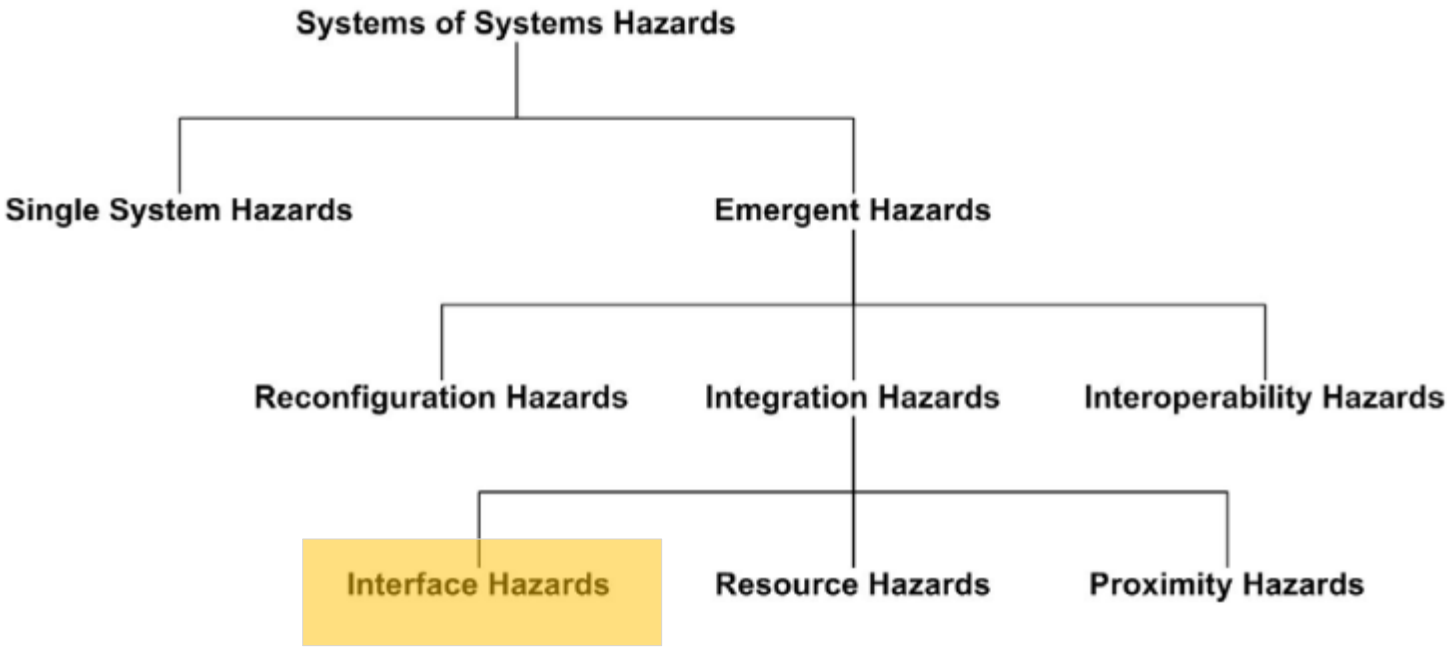
- Elements involved in site
- Who is exposed to site, who needs education or to be locked out?
- Foreseen Processes need to be described
- Critical areas to be defined

Worker at working Site
Operator Machine Excavator
Operator Machine Wheel Loader
Maintenance Team
Authorities
Publicity / Media
Emergency Rescue Services / Fire Fighters
HX
Other Machines, Equipment



Insights

What types of Hazards can be identified?



Redmond et al., ” Interface Hazard Analysis for System of Systems”, SOSE 2008

Challenge

How to connect to safety processes?

- STPA does not use quantification (SIL, ASIL) of hazards, unsafe control actions
- STPA connected to RAMS process – first approaches: ”Combining System-Theoretic Process Analysis and availability assessment: a subsea case study”, Juntao Zhang, HyungJu Kim, Yiliu Liu, Mary Ann Lundteigen
- Question how to connect the results to existing processes in industry?

6. Future Directions

- Providing input to analysis
  - Scenarios
  - Behavior
- Reconfigurations
- Scalibilty

Thank You!

stephan.baumgart@volvo.com