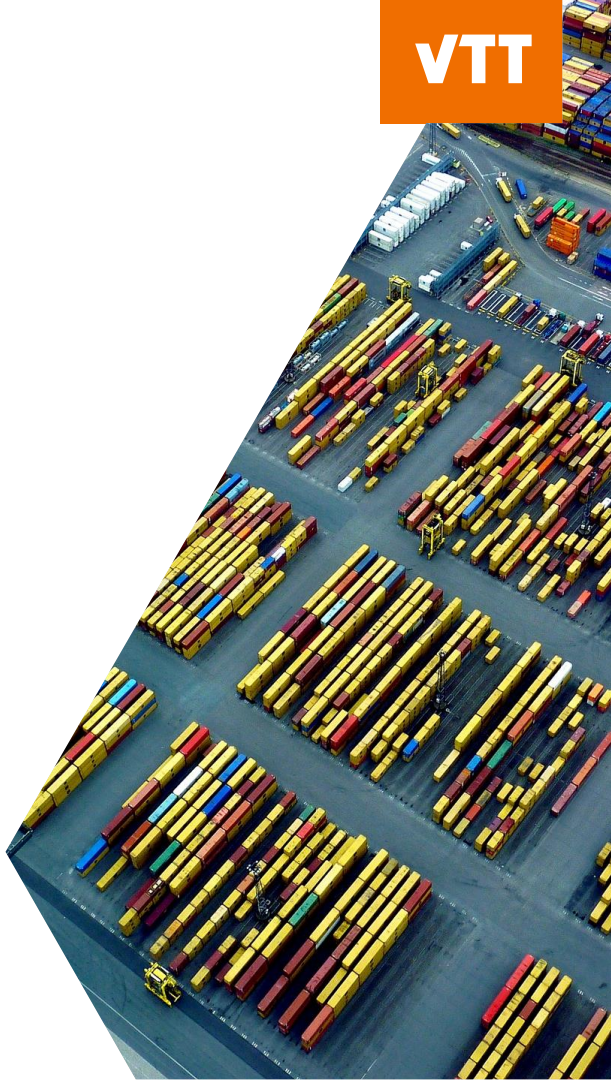
Applying STPA in development of autonomous container handling machinery

Eetu Heikkilä, eetu.heikkila@vtt.fi
Timo Malm, timo.malm@vtt.fi
Janne Sarsama, janne.sarsama@vtt.fi
Risto Tiusanen, risto.tiusanen@vtt.fi

VTT Technical Research Centre of Finland Ltd.

Introduction

- AUTOPORT project (https://autoport.fi) studies digital technologies and automation in port terminals
- We have studied the applicability of STPA in the development of autonomous container handling machinery, and compared the method with HAZOP.
- This presentation consists of:
  - Evaluation categories for comparing hazard analysis methods in the context of autonomous mobile machinery.
  - Findings of a case study applying STPA and comparison with HAZOP.



Automation in port terminals: towards autonomy

- Increasing level of automation is a global trend.
- Highly automated port terminals already exist in large seaports. Safety is addressed by placing automated machinery in areas fully separated from other traffic.
- Now also smaller ports are looking for improved efficiency using increasingly automated and even autonomous systems.
  - To maintain flexibility of operations, separation from other traffic is not possible.
  - This introduces new mixed-traffic situations involving autonomous and manually operated machines and humans → new hazards need to be considered.

System-level safety considerations

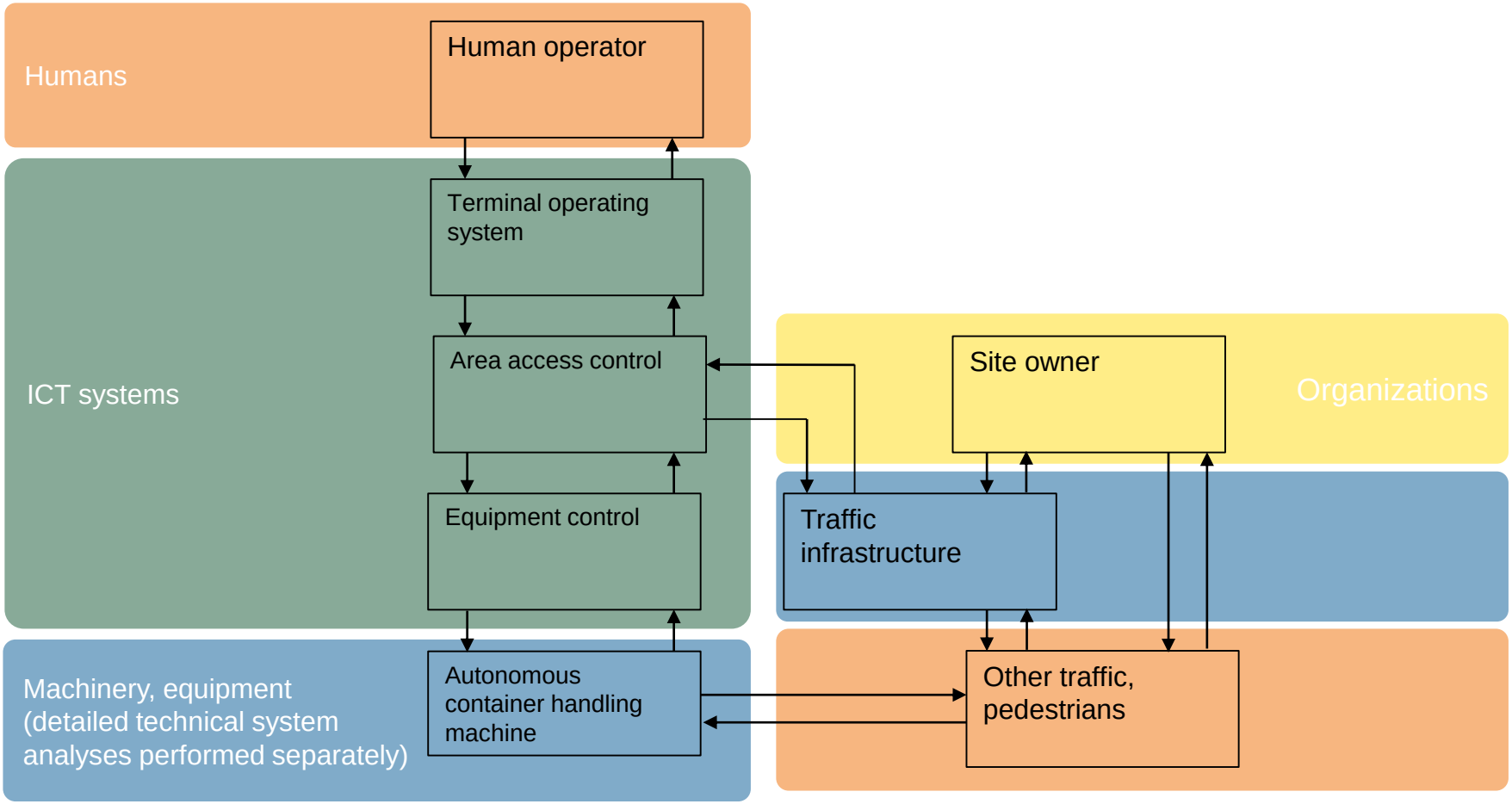
- The port environment is a complex socio-technical system consisting of several elements, including:
  - Automated and manually operated machinery
  - Other traffic
  - Workers representing several organizations
  - ICT systems
  - etc…
- Often the safety issues are related not only to the operation of the automated machine, but to the integration of these different elements.
  - Traditional machinery safety methods do not fully cover identification of these issues → potential application area for STPA.

Comparison of hazard analysis methods

- Categories applied in the evaluation of STPA applicability and comparison with HAZOP:

C-1 Capability to discover unique autonomy-related hazards
C-2 Scope and limitations of the analysis
C-3 Quality and characteristics of the analysis output documentation
C-4 Expertise and knowledge of the method required to perform analysis
C-5 Approach to system modelling and required background documentation
C-6 Tools and work methods suitable for carrying out the analysis
C-7 Need for other analysis methods

System elements (simplified excerpt from STPA)



Findings from autonomous operation STPA case study and HAZOP comparison (1/2)

- For the most part, STPA and HAZOP identified similar hazards, many of which were related to timing or order of commands (supported by guide words).
- STPA emphasizes consideration of the context (e.g. different operational modes or situations), leading to more descriptive scenarios than HAZOP.
- HAZOP focuses only on deviations, whereas STPA also looks at issues in the intended operation.
- STPA focuses the analysis activities efficiently, whereas HAZOP identifies any deviations – also ones with no significant effects.

Findings from autonomous operation STPA case study and HAZOP comparison (2/2)

- In STPA, modelling of the control structure requires expertise but it can also provide better understanding of the system.
- In STPA, the defined syntax and heavily text-based nature of outputs ensure quality and consistency, but sometimes hinder the method's use as a group brainstorming tool.
- STPA requires deeper understanding of the method from the analysis participants. Skilled facilitator is needed in both analyses.
- Both STPA and HAZOP are identification methods (no risk ranking or prioritization).

Conclusions

- Automation in port terminals is progressing towards autonomy and mixed-traffic operations, introducing new safety issues.
- Our study represents one of the first applications of STPA in the heavy mobile machinery domain.
- We found STPA to be well suited for identification of hazards and accident scenarios related to increasing autonomy of machinery.
  - Other methods are still needed as well in machine system development, e.g. for functional safety.

https://autoport.fi

beyond

the obvious

Eetu Heikkilä
eetu.heikkila@vtt.fi
+358 40 849 5790

@VTTFinland

www.vtt.fi