Scientific Journal of Gdynia Maritime University

No. 125/23, 25–39
ISSN 2657-6988 (online)
ISSN 2657-5841 (printed)
DOI: 10.26408/125.02

Submitted: 23.11.2022
Accepted: 02.02.2023
Published: 31.03.2023

HAZARD ANALYSIS OF AN AUTONOMOUS CONTAINER HANDLING SYSTEM – A COMPARISON OF STPA AND HAZOP METHODS

Eetu Heikkilä[1*], Timo Malm[2], Janne Sarsama[3], Risto Tiusanen[4], Toni Ahonen[5]

[1,2,3,4,5] VTT Technical Research Centre of Finland Ltd., Tekniikantie 21, Espoo, Otaniemi, Finland

[1] e-mail: eetu.heikkila@vtt.fi, ORCID 0000-0001-8259-0996

[2] ORCID 0000-0003-1612-3139

[3] ORCID 0000-0002-3569-4634

[4] ORCID 0000-0002-8717-7727

*Corresponding author

Abstract: Increasing automation is a major trend in container terminals. In automated container handling systems, safety has been previously ensured by segregating the automated machinery from other traffic and workers moving on foot. Currently, further increases in flexibility are sought by developing autonomous systems that are capable of mixed-traffic operations without the need for separate operating areas. This increases the complexity of the systems and introduces new safety hazards. In addition to traditional hazard analysis methods, new approaches are needed to address the emergent risks related to autonomous operations. This paper studies the applicability of the STPA (system-theoretic process analysis) method in hazard analysis of an autonomous machine system. To support the evaluation, we define evaluation categories for comparison of the analysis methods. We also compare STPA with an established method, HAZOP (hazard and operability study). To perform the comparison, both STPA and HAZOP are applied to an autonomous container handling system concept. The study suggests that both STPA and HAZOP are well suited to support the development of autonomous machinery. However, we also highlight some notable differences in the methods, mostly related to the different underlying accident models that they utilise. HAZOP is an established method with tools and standards available. STPA, on the other hand, provides a well-defined syntax to ensure the analysis quality and a system modelling approach that supports the system development.

Keywords: hazard analysis, autonomous systems, safety engineering, STPA, HAZOP.

1. INTRODUCTION

The automation of container terminals has been increasing starting from the mid to late 1990s, with large seaports driving the development towards automated operations [Heilig, Schwarze and Voss 2017; Gekara and Thanh Nguyen 2018].

Large ports have been able to improve efficiency by investing in entire automated terminals, where the automated machines operate separated from the other traffic and people working in the port area. In recent years, smaller ports, which operate mostly with manually operated machinery, have also shown increasing interest in automation. In small ports, however, investment in separate automated terminals is not feasible. Instead, the machinery applied in such cases would need to be autonomous so they are capable of flexible operations in an open setting involving manually operated machines, road vehicles, and workers moving on foot.

Ensuring safety in an open autonomous system is a much more complicated task than in situations where the automated operating area is fenced off [Heikkilä et al. 2020]. When autonomy increases, the systems become increasingly complex, interconnected, and involve new kinds of human-automation interfaces [Karvonen, Heikkilä and Wahlström 2020]. This increases the number of interactions between system elements, leading to emergent and nonlinear behaviour that can be highly unpredictable [Kaloudi and Li 2021]. Thus, recent research suggests that accident models traditionally used in safety engineering, which are typically based on chains-of-failures or chains-of-events, are insufficient in the identification of safety issues that may arise in complex systems [Leveson 2012]. The advantages and limits of the traditional hazard identification methods, the state-of-the-art practices as well as needs for new approaches are discussed widely by, e.g., Baybutt (2021), Pasman et al. (2021) and Dghaym et al. (2021).

New safety analysis methods based on system theory, such as the system-theoretic process analysis (STPA) [Leveson and Thomas 2018], have been proposed as alternative approaches to support the identification of hazards. However, due to the relative novelty of these methods, their applications on industrial machinery systems have not been widely published in research literature. Thus, research is needed on their suitability in the mobile machinery sector.

This paper investigates the applicability of the STPA method in the development of new concepts for highly automated or autonomous mobile machinery. We address this question by comparing STPA with Hazard and Operability Study (HAZOP) i.e. one of the well-established hazard analysis methods. The main contributions of this paper are two-fold. First, we define evaluation criteria for comparing the methods in the context of autonomous machine systems. Second, we compare STPA with HAZOP using the defined criteria. This includes a review of the standards and instructions supporting the analysis activities, as well as case applications of both methods on an autonomous container handling system. HAZOP was selected for the comparison as it has been previously successfully applied in the development of new mobile heavy machinery systems, such as mining machinery and construction equipment [Tiusanen 2014; Muram, Javed and Punnekkat 2019].

2. BACKGROUND

2.1. Approaches to hazard identification

Traditional approaches applied in safety and reliability engineering are predominantly risk-based. There are several ways to define the concept of risk, but usually it is defined as a combination of the severity and probability of an undesired event [Aven 2010; Hafver et al. 2017]. Due to the issues in a solely risk-based approach, arguments have been presented against the use of traditional safety analysis methods, which often focus on analysis of component failures or linear chains of events, rather than identifying problems arising from unsafe interactions between system elements [Leveson 2012].

Providing an alternative to the risk-based approaches, STPA (Systems-Theoretic Process Analysis) is a relatively recent hazard analysis method based on STAMP (Systems-Theoretic Accident Model and Processes). STAMP is an accident causality model based on systems theory, considering safety as a control problem instead of focusing on failures or deviations. It describes the system as a hierarchical control structure consisting of feedback loops, intending to incorporate various causal factors, including software aspects, as well as human and organisational factors. STPA provides a systematic procedure to identify flaws within the safety control structure [Leveson 2012]. The STPA process has been described in the freely available STPA Handbook, which has seen several updates and revisions over the years (latest version by Leveson and Thomas, 2018). All the later references to the 'STPA Handbook' in this paper refer to this version of the document. The Handbook also provides definitions for the key concepts and terminology.

Leveson and Thomas (2018) define the method as follows: Step 1 defines the scope and limitations of the analysis. In Step 2, the system is modelled as a hierarchical control structure, which is a system model composed of feedback control loops. This is a graphical representation featuring controllers and controlled processes represented as rectangles, and the interactions between them (control and feedback) represented as arrows. The hierarchy is illustrated by the vertical axis, i.e., the highest control authority is at the top of the diagram. In Step 3, the control structure is systematically analysed to find unsafe control actions (UCAs) that, in a particular context and worst-case environment, will lead to a hazard. Finally, Step 4 concludes with the identification of loss scenarios, which describe the causal factors that can lead to UCAs and hazards.

The hazard and operability study (HAZOP) method, on the other hand, was initially developed in the early 1960s for the analysis of chemical process systems, but it has since been widely applied in other industrial sectors. The HAZOP analysis procedure is defined in international standard IEC 61882:2016 'Hazard and operability studies (HAZOP studies). Application guide'. In the later parts of this paper, this standard is referred to as the 'HAZOP standard'.

According to the HAZOP standard, the method is a structured and systematic technique for examining a defined system, with the objectives of identifying hazards associated with the operation and maintenance of the system and identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to non-conforming products.

In previous research, there are some existing studies where STPA has been compared to HAZOP. The domain areas of these studies include the process industry [Rodriguez and Diaz 2016; Sultana et al. 2019; Yousefi and Rodriguez 2019], and the railway and urban rail transit sectors [Yan, Tang and Yan 2016].

In the study by Bensaci, Zennir and Pomorski (2018), STPA was applied to a Complex Multi-Robot Mobile System. Furthermore, STPA has been compared with several methods other than HAZOP in several domains. One example is the maritime transport sector, where the development of autonomous vessels is progressing rapidly and has spurred the research on STPA and its relation to other methods [Basnet, Valdez Banda and Kujala 2018]. In the maritime sector, STPA has also been a basis for wider frameworks for autonomy development [Chaal et al. 2020; Dghaym et al. 2021]. In the heavy industrial mobile machinery sector, however, there are no published STPA studies known to the authors.

3. MATERIAL AND METHODS

The work related to the comparison of hazard analysis methods presented in this paper follows a comparative case study research approach. The aim of a comparative case study is to cover two or more cases to produce generalisable information – in this case, regarding the applicability of hazard identification methods in the given context. Comparative case study research focuses on the identification and analysis of similarities, differences, and patterns in two or more cases with a common focus or goal [Goodrick 2014].

Figure 1 visualises the research procedure applied in this paper. To evaluate the applicability of STPA for autonomous systems development and to provide comparisons with HAZOP, the first step of our research was the definition of categories to be used in the evaluation of the methods. This was followed by an investigation of the documentation that describes the analysis methods. The STPA and HAZOP analyses were carried out as separate case studies with separate analysis teams focusing on a container handling system.

The analyses were carried out by the following analysis teams:

- STPA: 3 researchers (all M.Sc., with several years of experience in traditional methods. One participant with previous experience in STPA facilitated the analysis);

- HAZOP: 2 researchers (M.Sc. and D.Sc., with several years of experience in HAZOP and other traditional methods).

To coordinate the case studies, the detailed definition of the case system and its boundaries were defined in co-operation between the analysis teams so that both the STPA and HAZOP were conducted using the same system definition and at a similar level of detail. Thus, some exchange of ideas between the analysis teams happened at the beginning. The time taken to carry out the analyses was similar for both HAZOP and STPA. Based on these studies, conclusions on the key characteristics and applicability of the methods were provided.

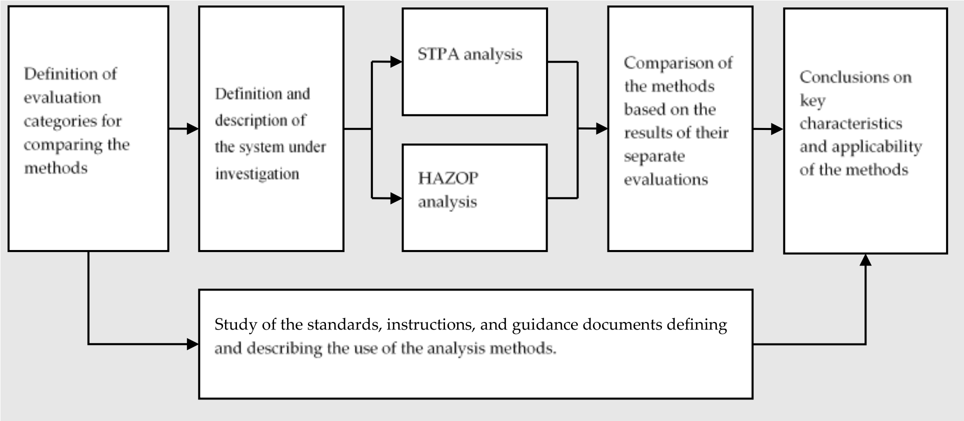
Definition of evaluation categories for comparing the methods
Definition and description of the system under investigation
STPA analysis
HAZOP analysis
Comparison of the methods based on the results of their separate evaluations
Conclusions on key characteristics and applicability of the methods
Study of the standards, instructions, and guidance documents defining and describing the use of the analysis methods.

Fig. 1. Overview of the research procedure followed in this paper

Source: own study.

3.1. Evaluation categories for comparing the methods

Analysis methods and their applicability can be evaluated from various perspectives. In our case study, the focus was on the ability of the methods to identify new risks related to autonomy. Additional points of interest included the efficiency of analysis activities, guidance provided by the method, as well as the quality of the analysis outputs. Based on these needs, evaluation categories were defined.

The categories presented in Table 1 consist of factors that deal with the analysis process itself, as well as the characteristics of the analysis outputs. The evaluation categories are intended for qualitative analysis, i.e., the findings related to the performance of the methods are not based on quantitative values (such as the number of scenarios identified or time resources taken), but rather on the experiences of the analysis participants.

Table 1. Evaluation categories for comparison of the hazard analysis methods developed for and applied in this study

Category	Description
C-1 Capability to discover unique autonomy-related undesired scenarios	What are the differences in the number and types of hazards identified by the methods? The hazards identified were studied in detail to assess whether their discovery was clearly supported by the method used, and to evaluate whether the hazard would have been unlikely to be discovered with the other method.
C-2 Scope and limitations of the analysis	What guidance is provided for defining the analysis subject?
C-3 Quality and characteristics of the analysis output documentation	What are the products that the analysis produces and what guidance is provided for creating the documentation?
C-4 Expertise and knowledge of the method required to perform analysis	How much expertise does the analyst require to be able to perform the analysis?
C-5 Approach to system modelling and required background documentation	What type of system model does the analysis use, and what information is needed to successfully perform the analysis?
C-6 Tools and work methods suitable for carrying out the analysis	How is the analysis instructed to be facilitated, and what are the best work practices for conducting the analysis? What tools are available for facilitation?
C-7 Need for other analysis methods	Does the analysis method need to be complemented by other analyses? If so, how well is the analysis method aligned with the other methods?

Source: own study.

3.2. System under investigation in cases

The target system for experimenting with hazard analysis methods is a container handling machine application where an autonomous shuttle carrier transports containers following certain roads, utilising specific loading and unloading areas for container handling. The machine fleet consists of several shuttle carriers operating at the same time using the same roads. The overall logistic operation is controlled by the terminal operating system (TOS) and the automated shuttle carrier fleet is controlled by the Equipment Control System (ECS). The operating environment, roads and container handling areas are monitored, and the Area Access Control System (AAC) controls access to the terminal area. The automatic driving is implemented in stages so the ECS provides information on the next part of the route and the associated boundary conditions. The operating principle of the automated shuttle carrier fleet is based on the ‘Mixed traffic’ operating concept where the automated carriers, manual work machines and trucks, as well as workers moving on foot or bicycle use the same roads simultaneously.

Figure 2 describes the system elements that were included in the STPA and HAZOP analyses.

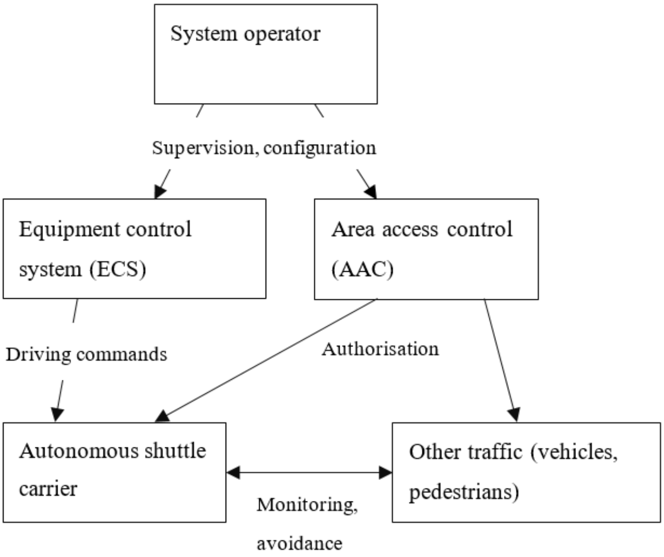
System operator
Supervision, configuration
Equipment control system (ECS)
Area access control (AAC)
Driving commands
Authorisation
Autonomous shuttle carrier
Other traffic (vehicles, pedestrians)
Monitoring, avoidance

Fig. 2. Overview of the system analysed with HAZOP and STPA

Source: own study.

4. RESULTS

Both STPA and HAZOP were applied on the system described above and the analysis activities considered in this paper focused on the system elements depicted in Figure 2. The following subsections describe the findings of the comparative study of the analysis methods. The results are structured as subsections, following the evaluation categories presented in Table 1. Further conclusions of the comparison are then presented in the discussion section.

4.1. Capability to discover unique autonomy-related undesired scenarios

The focus of the analyses carried out was the new risks that emerge from autonomous operation of machinery in an open operating environment. Generally, STPA and HAZOP were found to support the identification of mostly similar scenarios, as many of the findings related to autonomy are based on correct timing or order of commands. The similarities in the findings are mainly due to the similarities in the categories and guide words that the analysis methods use. In STPA, the categories are related to control actions and there are four fixed categories for identification of unsafe control actions. These categories are 'not providing causes hazard', 'providing causes hazard', 'too early, too late, out of order', and 'stopped too soon, applied too long'. STPA Handbook claims that this is a complete listing in all cases, but also states that subcategories should be considered.

In HAZOP, the analysis team decides the guide words, but typically they are very similar to the categories in STPA. The HAZOP standard provides examples of guide words, such as 'more', 'less', 'early', and 'late'. There is no limit to the number of guide words and the analysis team may use additional guide words not mentioned in the standard, as long as they are decided before the analysis. This may provide the possibility to define guide words that support the definition of autonomy-related hazards better than the preset guide words in STPA. However, no such guide words were identified in our case application. Generally, issues related to timing (e.g. delayed commands or commands in the wrong order) were well identified with both HAZOP and STPA.

A clear distinction between HAZOP and STPA is related to the differences of the fundamental accident models behind the analyses. HAZOP is based on a model where accidents are caused by the presence of deviations in system elements from their design intent. Thus, the method assumes that the intended functionality of the system itself does not cause accidents. Therefore, it does not support the identification of design-related issues in the intended functionality. STPA, on the other hand, assumes that accidents are caused by a lack of control. Thus, it can support considerations where the system is operating as designed, but still causes a hazard in some conditions. STPA also considers the feedback on whether the command was properly executed. In HAZOP, this may be overlooked as the focus is on deviations.

The consideration of context is an important feature in STPA also from the perspective of considering other aspects of the system, such as environmental conditions. In HAZOP, this is not emphasised. In STPA, the scenarios that are created as a result of the analysis always include a context.

4.2. Scope and limitations of the analysis

Hazard analyses typically start with the definition of the object of analysis and the boundaries of the system that is being studied. In the HAZOP standard, general guidance is given for setting the scope and limitations of the analysis. In practice, the standard states that 'the boundaries and extent of the system' need to be defined, as well as the level of detail on which the analysis is carried out. Additionally, previous studies and existing regulations and standards need to be considered. The HAZOP standard also ties the analysis into the organisational objectives and safety and performance requirements of the system in terms of the organisation's business.

In STPA, the first step of the analysis procedure is titled 'Definition of the analysis purpose' and it also essentially focuses on setting the scope and limitations. First, the analyst defines the losses that the analysis is to focus on. Losses can be defined freely based on what is seen to be of value to stakeholders. Using the word 'loss' could also avoid confusion between different industries, where several words, such as accidents or mishaps, are used. The STPA Handbook provides guidance for the definition of losses stating from identification of the stakeholders and their values and goals regarding the system. In STPA, losses are generally defined at a high level and include aspects such as 'Loss of life or injury to people' and 'Loss of or damage to vehicle'. The losses do not need to be limited to safety: aspects such as production loss or reputation loss can also be considered.

The next part of STPA step 1 involves the definition of system-level hazards. This also includes the definition of the system boundaries. The STPA Handbook states that the boundary can be defined by considering the parts over which the system designers have control. The STPA Handbook emphasises that system-level hazards are indeed system states or conditions, and component-level aspects should not be considered at this point.

In conclusion, both HAZOP and STPA include a phase that focuses on setting the scope and limitations. In HAZOP, this is clearly included in the standard approach, but rather limited guidance is given to the analyst on how to define the scope. In STPA, the defined process can support in focusing the analysis activities. Typically, the focus in STPA is set on worst-case situations, whereas HAZOP will identify any deviations, including ones without significant consequences. Thus, by default, STPA can be seen to support more efficient resource allocation of the analysis activities, assuming that step 1 is properly conducted.

4.3. Quality and characteristics of the analysis output documentation

All analyses aim for clear documentation, but there are different approaches to how the analysis methods direct the documentation and its structure. Both STPA and HAZOP are qualitative methods. Additionally, they do not offer guidance for prioritisation of the identified hazards.

In HAZOP, the result of the analysis is typically a report containing the analysis background and the analysis findings. The analysis findings are collected in a worksheet or in a specific piece of software. The HAZOP standard provides the titles for the columns that should be included in a worksheet, but no detailed definitions on how the information should be expressed.

In STPA, there are different types of analysis outputs, including unsafe control actions (UCAs) and loss scenarios. The loss scenarios are the final output of the analysis. They are text-based descriptions of accident scenarios, describing the involved system elements, as well as the cause and context that can lead to an accident. The STPA Handbook provides some guidance for identifying different types of loss scenarios. This part of the analysis, however, is not backed up with such a defined process as the earlier phases of the STPA analysis. To support identification of the loss scenarios, industry-specific guidance such as checklists would be beneficial, as long as they are applied in the process, so they do not narrow the considerations of the analysis participants.

STPA enforces a pre-defined syntax for several elements that are recorded in the analysis process. For example, in step 1, a specific syntax is given for how the system-level hazards should be formulated. It also includes linking to the losses identified earlier in the analysis, supporting traceability of the analysis results. Similarly, in later stages of the analysis, UCAs and loss scenarios are formulated according to a specified syntax and with relevant linking for traceability.

Due to the specified syntax in most parts of the analysis, STPA enforces the documentation of analysis findings in a way that is consistent and easily comprehensible when reviewed by someone who did not participate in the analysis. On the other hand, the results are heavily text-based, and not suitable for acquiring a quick overview of the most important safety issues. The defined syntax can also increase the workload of the analysis. In HAZOP, the documentation is much more subject to the personal preferences of the person documenting the findings.

4.4. Expertise and knowledge of the method required to perform the analysis

The use of different hazard analysis methods does not replace the need to understand the system being studied. Thus, when assessing this factor, we focused only on the analysis methods and assumed that anyone participating in the analyses has a sufficient technical understanding of the system under study.

In HAZOP, the success of the analysis is strongly dependent on the competence of the analysis facilitator. The experts involved in the analysis are required to have a good understanding of the system that is being studied, but they do not need to be experienced in HAZOP as a method, as the facilitator guides the process. Even for analysis group members unfamiliar with HAZOP, the concept of deviations is fairly easy to understand.

Based on the analysis cases carried out, STPA requires, when compared to HAZOP, a significantly deeper understanding of the method itself and the underlying system-theoretic perspective on safety. STPA introduces several concepts and novel terminology, such as system-level hazards and loss scenarios. The analysis participants need to understand these concepts to be able to formulate the analysis outputs correctly. Additionally, development of the safety control structure diagram requires an understanding of the basic concepts of control engineering and feedback loops. It also requires expertise to formulate the model so that all relevant elements are included. An experienced facilitator can support this to some extent.

4.5. Approach to system modelling and required background documentation

Hazard analysis is based on the understanding of the system that can be acquired from design documentation and experts involved in the system development. Based on this information, different analysis methods employ various approaches to model the system to support the analysis. HAZOP typically uses the technical documentation available in the system, such as circuit diagrams or piping and instrumentation diagrams. The HAZOP standard states that ‘accurate and complete design representation’ is required to carry out the analysis. This documentation is then systematically reviewed in the analysis process. If HAZOP is used at a less detailed (e.g. functional) level, some other type of system functional description can be used.

In STPA, such prerequisites for system documentation are not provided. The analysis can be based on any information of the system, but according to our case study, it is very difficult to formulate the safety control structure without a detailed system description. On the other hand, this would suggest that STPA can be a useful tool in supporting system design, as it can point out parts of the system where the control structure is not yet defined, and to guide the design.

A major difference between the two methods is that, in STPA, a specific system model is always created. The model represents the safety control structure, depicting the system elements, their interactions, and the control hierarchy. The creation of the system model was found to be useful: it supports the system design by visualising the interactions between system elements and possible deficiencies in these. However, the system modelling also requires additional resources and expertise to be able to define it at a suitable level of detail. According to the STPA Handbook, the goal is to manage the complexity by applying abstraction in the control structure. This makes it very challenging to evaluate the control structure model, i.e., to ensure that all the needed elements are in place and modelled with an appropriate level of detail for an acceptably thorough analysis.

4.6. Tools and work methods suitable for carrying out the analysis

HAZOP is, by definition, a group analysis method. It should be carried out with a trained and experienced facilitator leading the analysis. The study itself utilises the expertise of a selected team of specialists with relevant experience of the system being analysed. Each member of the analysis team has a specific role defined at the start of the analysis process.

The STPA Handbook analysis description does not provide detailed guidance for the actual facilitation of the analysis. However, it does include a chapter on how to introduce STPA in an organisation. This section also covers the roles and training of the people involved in the analyses. It encourages that a facilitator should be used in a similar fashion as in HAZOP. It is stated that STPA is best performed as a small group exercise. According to our findings, however, the heavily text-based nature of the documentation sometimes hinders effective group work.

In both HAZOP and STPA, the analysis results are typically recorded with a software application, ranging from templates in office programs to sophisticated software with broad project management capabilities. As HAZOP is a widely used and standardised method, specific software tools have been available for a long time. For STPA, the amount of available software tools is smaller as the method is newer and currently not as widely used. However, both open source and commercial implementations for STPA are available. For this paper, both STPA and HAZOP analyses were conducted using widely available general office software tools, leaving detailed evaluation of the features of analysis-specific software tools outside the scope of our study.

4.7. Need for other analysis methods

In system safety engineering, different methods are often used in combination to achieve comprehensive results. The HAZOP standard provides some examples of how the analysis can be complemented by other methods where necessary. Specifically, it suggests that a component-level failure modes and effects analysis (FMEA) can be used when HAZOP identifies components that are critical for the system performance. Additionally, it is suggested that fault tree analysis (FTA) or event tree analysis (ETA) can be used to quantify the likelihood of events identified by HAZOP.

In the STPA Handbook, no other analysis methods are suggested to be used in conjunction with STPA. Instead, the Handbook claims that in all evaluations where STPA has been compared with traditional methods (such as FTA, ETA, FMECA, or HAZOP), STPA has always been able to identify all the causal scenarios identified by the other methods as well as many others that the traditional methods were not able to identify. The Handbook also claims that STPA is more resource efficient as well. However, no direct references are provided to defend these claims.

5. CONCLUSIONS

Hazard identification methods have been developed and applied for a long time in industry. Because of the increasing complexity of industrial systems, there is need for more holistic ways to identify hazards using a socio-technical system approach, lifecycle approach, and new analysis methods such as STPA and formal modelling.

This paper studied the applicability of STPA in the development of autonomous machinery and presented a comparative study of STPA and HAZOP analyses applied on an autonomous container handling system. The results suggest that both STPA and HAZOP are suitable methods to be applied in the development of autonomous machinery, as they both address relevant issues related to the timing and correctness of information transferred between different system elements. However, we also identified some notable differences between the methods.

The first contribution of this paper was the definition of the evaluation categories for comparison of the methods. These categories were formulated based on needs identified in research and development projects related to machinery. Various comparisons of hazard analysis methods have been published in previous research. However, these studies are not necessarily related to machinery, nor do they follow pre-defined categories to structure the findings.

Currently, the evaluation categories presented in this paper are qualitative and they focus on the development of autonomy. However, they can be modified to support broader comparisons of hazard analysis methods in the machinery sector. Further research can be considered to elaborate on the categories, for example, to include quantitative aspects to evaluate the efficiency of different methods.

The second contribution of this paper focused on a comparison of STPA and HAZOP. In the research literature, the applicability of STPA in the heavy mobile machinery domain has not been previously reviewed. However, we identified several studies where STPA has been applied in other domains and compared with other analysis methods. Based on the previous studies examined, we were not able to draw very far-reaching conclusions about the relationship between the STPA and HAZOP methods, i.e., whether one of the methods is clearly better than the other, or whether one can even replace the other. Both methods are qualitative and lack a quantitative analysis, which requires combining them with other analysis techniques.

Most of the previous studies found STPA useful, noting similar benefits to those we identified in our study. On the other hand, our findings are also in line with earlier experiences described by the process industry [Dghaym et al. 2021] that there are several issues that need to be addressed to get the best outcome from applying STPA. However, it is observed that STPA has unique positive features compared to HAZOP, and it is thus complementary to HAZOP, and can possibly even replace HAZOP entirely. Based on both our work and previous research, more research work is however needed to be able to answer this specific question and more general questions related to the relationship between these two methods.

In our STPA-HAZOP comparison, the major differences between the methods were related to the differences in the underlying accident models in these methods. STPA, when applied early in the development process, can be more efficient and better support the overall system development activities. However, it also requires that the analysis participants have a good understanding of the method itself. A skilled facilitator is essential in both analyses. This was also expressed by Dghaym et al. (2021) especially when building strong safety arguments.

The case application of STPA presented in this paper is one of the first published applications of the STPA method in the industrial mobile machinery sector. Thus, while the results are encouraging and suggest that STPA is a suitable approach for hazard identification in the development of autonomous machinery, further research is needed to gain experiences of its application in different phases of the design lifecycle and at various levels of detail.

6. ACKNOWLEDGEMENTS

Research on safety engineering methods and safety requirement management in autonomous machinery systems has been done and is ongoing in Finland in national co-innovation projects financed by Business Finland, VTT and participating companies.

REFERENCES

Aven, T., 2010, *On How to Define, Understand and Describe Risk*, Reliability Engineering and System Safety, vol. 95, no. 6, pp. 623–631.

Basnet, S., Valdez Banda, O., Kujala, P., 2018, *Review of the Safety Engineering Techniques for a Complex Ship System*, The 7th Asia Conference on Earthquake Engineering, Bangkok, Thailand.

Baybutt, P., 2021, *On the Need for System-Theoretic Hazard Analysis in the Process Industries*, Journal of Loss Prevention in the Process Industries, vol. 69.

Bensaci, C., Zennir, Y., Pomorski, D., 2018, *A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The Case of a Complex Multi-Robot Mobile System*, 2nd European Conference on Electrical Engineering and Computer Science, EECS, Bern, Switzerland, 20–22 December 2018, IEEE, New York, USA.

Chaal, M., Valdez Banda, O., Basnet, S., Glomsrud, J.A., Hirdaris, S., Kujala, P., 2020, *A Framework to Model the STPA Hierarchical Control Structure of an Autonomous Ship*, Safety Science, vol. 132.

Dghaym, D., Hoang, T.S., Turnock, S.R., Butler, M., Downes, J., Pritchard, B., 2021, *An STPA-Based Formal Composition Framework for Trustworthy Autonomous Maritime Systems*, Safety Science, vol. 136.

Gekara, V.O., Thanh Nguyen, V.X., 2018, *New Technologies and the Transformation of Work and Skills: A Study of Computerisation and Automation of Australian Container Terminals*, New Technology, Work and Employment, vol. 33, no. 5, pp. 219–233.

Goodrick, D., 2014, *Comparative Case Studies: Methodological Briefs: Impact Evaluation No. 9*, UNICEF Office of Research, Florence, Italy.

Hafver, A., Eldevik, S., Jakopanec, I., Drugan, O.V., Pedersen, F.B., Flage, R., Aven, T., 2017, *Risk-Based Versus Control-Based Safety Philosophy in the Context of Complex Systems*, Safety & Reliability, Theory and Applications, CRC Press, Boca Raton, FL, USA.

Heikkilä, E., Malm, T., Tiusanen, R., Ahonen, T., 2020, *Safety and Dependability of Autonomous Systems in Container Terminals: Challenges and Research Directions*, Proceedings of the 6th International Conference on Vehicle Technology and Intelligent Transport Systems, VEHITS 2020, SciTePress, Setúbal, Portugal.

Heilig, L., Schwarze, S., Voss, S., 2017, *An Analysis of Digital Transformation in the History and Future of Modern Ports*, Proceedings of the 50th Hawaii International Conference on System Sciences, HICSS 2017.

Kaloudi, N., Li, J., 2021, *Comparison of Risk Analysis Approaches for Analyzing Emergent Misbehavior in Autonomous Systems*, Proceedings of the 31st European Safety and Reliability Conference ESREL 2021, Angers, France.

Karvonen, H., Heikkilä, E., Wahlström, M., 2020, *Safety Challenges of AI in Autonomous Systems Design – Solutions from Human Factors Perspective Emphasizing AI Awareness*, Engineering psychology and Cognitive Ergonomics. Cognition and Design: HCII 2020, Springer, Cham, Switzerland.

Leveson, N., 2012, *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge, MA, USA.

Muram, F.U., Javed, M.A., Punnekkat, S., 2019, *System of Systems Hazard Analysis Using HAZOP and FTA for Advanced Quarry Production*, 4th International Conference on System Reliability and Safety, ICSRS 2019, Rome, Italy, IEEE, New York, USA.

Rodríguez, M., Díaz, I., 2016, *System Theory Based Hazard Analysis Applied to the Process Industry*, International Journal of Reliability and Safety, vol. 10, no. 1, pp. 72–86.

Saurí, S., Morales Fusco, P., Martín, E., Benítez, P., 2014, *Comparing Manned and Automated Horizontal Handling Equipment at Container Terminals*, Transportation Research Record: Journal of the Transportation Research Board 2014, no. 2409, pp. 40–48.

Sultana, S., Okoh, P., Haugen, S., Vinnem, J.E., 2019, *Hazard Analysis: Application of STPA to Ship-to-Ship Transfer of LNG*, Journal of Loss Prevention in the Process Industries, vol. 60, pp. 241–252.

Tiusanen, R., 2014, *An Approach for the Assessment of Safety Risks in Automated Mobile Work Machine Systems*, Dissertation, VTT, Espoo, Finland.

Yan, F., Tang, T., Yan, H., 2016, *Scenario Based STPA Analysis in Automated Urban Guided Transport System*, 2016 IEEE International Conference on Intelligent Rail Transportation, ICIRT, Birmingham, UK, 23–25 August 2016, IEEE, New York, USA.

Yousefi, A., Rodriguez, M., 2019, *Using a System Theory Based Method (STAMP) for Hazard Analysis in Process Industry*, Journal of Loss Prevention in the Process Industries, 2019, vol. 61, pp. 305–324.

Internet sources

Leveson, N., Thomas, J., 2018, *STPA Handbook*, https://psas.scripts.mit.edu/home/get_file.php?name=STPA_Handbook.pdf (accessed 18.08.2022).