Assessing an automated mining operation with STPA

Berger J[1]., Tiusanen R[1]., Malm T[1].

1 VTT Technical Research Centre of Finland

KEYWORDS: Systems-Theoretic Process Analysis, mine automation industry, system safety

ABSTRACT

Autonomous mining reshapes contemporary mining practices as it plays an increasing role in bringing value to customers. The benefits encompass improvements in operational efficiency, safety, and process reliability while offering flexible maintenance programs that reduce downtime and costs. Mine automation systems cover a wide range of automation, from individual control cabinets to controlling entire fleets. However, the growing complexity and functionality of these systems introduce new risks, necessitating a comprehensive safety analysis. Traditional hazard analysis methods, which examine system components separately and in isolation, are no longer adequate. In complex systems, such as mine automation systems, losses may occur not only due to component failures but rather because of unpredictable and undesired interactions among system elements. Rooted in system-theory, Systems-Theoretic Process Analysis (STPA) can address this complex, non-linear way of how losses can arise.

This study employs STPA to examine its suitability for the mine automation industry by assessing a mining pit's automated and remotely operated drill rig fleet. Additionally, the research explores the potential of STPA for identifying system requirements and safety goals in the context of mine automation systems. System elements of the examined use case are three automated drill rigs and a teleoperation station. The analysis deals with a typical daily maintenance use case when the mode of operation must be changed as the maintenance person approaches the drill rig and returns.

STPA, is implemented in four stages: defining the analysis' purpose, modelling the control structure, identifying the unsafe control actions, and finally describing loss scenarios. In comparison to traditional hazard and safety analysis tools, STPA gives special attention to control actions by dedicating Step 3 to identifying how assumingly suitable and safe control actions can become unsafe.

Results show that STPA, which views safety as a control problem, provides valuable insights into the dynamic interactions between the remote operator in the teleoperation station and the on-site maintenance personnel using the drill rig's onboard control system and the control cabinet at the site. The use-case analysis of six control actions revealed 15 possible unsafe control actions and over 40 possible loss scenarios. A significant share of loss scenarios is related to human - machine interactions. Concretely, the study highlighted the importance of communication between the maintenance person and the remote operator, emphasizing the need to prevent communication and connectivity problems. Additionally, challenges related to the indication of the operating mode of the drill rig and its transition as well as the location of on-site control cabinet affecting safety were identified. Proposals were made for clearer communication through clearer operating mode indication. Further, better site overview and visibility could prevent unintended drill rig approaches during drill rig's automatic operation. While the results are not of technical nature, they can aid in creating a safe work environment and understanding factors affecting the work at the site. STPA proved to deliver valuable input for discussions during system's conceptual design phase. Furthermore, the tool appears to contribute to assessing planed system design modifications as well as reassessing already existing systems.

This research has been conducted as a part of the "Future Electrified Mobile Machines" (FEMMa) project, which is mainly funded by Business Finland.

1 INTRODUCTION

Many today's societal and economic value chains involve the use of heavy working machines (WM), such as those found in mining and construction, agriculture, forestry, and material handling logistics. Leveraging recent advancements in digital technology, the WM industry has integrated automated functions and autonomous features. Consequently, the increasingly autonomous mining sector is reshaping contemporary mining practices and plays an important role in bringing value to customers. [1]

Traditional mining practices are shaped by the performance of tedious and repetitive tasks for prolonged hours leading to physical strain and fatigue among miners. Additionally, exposure to extreme conditions such as the constant threat of rock sliding, ground collapse, and the inhalation of excessive dust posed serious health hazards. These challenging working conditions not only compromise the safety of mining personnel but also make recruitment in the industry challenging. [2], [3]
However, benefits of modern, automation-enhanced mining practices encompass improvements in operational efficiency, safety, and process reliability while offering flexible maintenance programs that reduce downtime and costs. Mine automation systems cover a wide range of automation, from individual control cabinet to controlling entire fleets. The degree of autonomy pursued is dependent on the objectives, opportunities, and requirements imposed by the operating environment. The shift towards increased machine autonomy will significantly impact the nature of work tasks and roles at mining sites. For example, manual drivers will cooperate with automated or autonomous WM at the site, or transition to roles as remote operators or system operators located in control rooms. [1]

Implementing advanced operating concepts that allow autonomous WM, manual machines, and workers to operate and collaborate in the same open work area pose challenges. The growing complexity and functionality of these systems introduce new risks, necessitating a comprehensive safety analysis.

Despite being well established in industry, traditional hazard analysis methods (Preliminary Hazard Analysis (PHA), fault tree analysis (FTA), failure modes and effects criticality analysis (FMECA), event tree analysis (ETA), and hazard and operability analysis (HAZOP)) fall short in adequately identifying risks associated with complex systems. These methods typically involve examining system components separately and in isolation, concentrating on identifying failures, faults, and their effects on single system level. [4] However, in complex systems, such as mine automation systems, losses may not only occur due to component failures but rather because of unpredictable and undesired interactions among system elements. Rooted in systems-theory, Systems-Theoretic Process Analysis (STPA) can address this complex, non-linear way of how losses can arise [5].

In this study, we applied STPA to gain practical experience, and evaluate the applicability of STPA for automated mining operations. Therefore, we assessed the operation of automated and remotely operated drill rigs in a mining pit when a human is nearby. The analysis explores a use-case regarding a typical daily maintenance task. In this scenario, the mode of operation must be adjusted upon the maintenance person's approach to and return from a drill rig. The system under investigation includes three automated drill rigs and a teleoperation station. Additionally, the study explores the potential of STPA for identifying system constraints, requirements, and safety goals in the context of mine automation systems.

2 STPA

In the early 2010s, Leveson at MIT (Massachusetts Institute of Technology) introduced a novel, qualitative safety analysis method known as Systems-Theoretic Process Analysis (STPA) to address system-based hazards. STPA draws its foundation from Systems-Theoretic Accident Model and Processes (STAMP) which considers non-linear relationships of technical and organizational structures, design and requirements flaws, as well as dysfunctional interactions between components that each individually act as intended. Unlike traditional views that assign unwanted scenarios to hazardous events and simple chains of failure events, the systems theory recognizes systems' dynamic properties and complex interactions. It acknowledges that system elements engage and impact each other, leading to the emergence of new, non-obvious pathways for accidents.[5], [6], [7]

STPA, treating safety as a dynamic control problem is tailored for complex systems and exposes unsafe control commands that one system element could have upon another. The method is implemented in four stages:
defining the analysis' purpose, modelling the control structure, identifying the *unsafe control actions* (UCA), and finally describing *loss scenarios* (Figure 1).

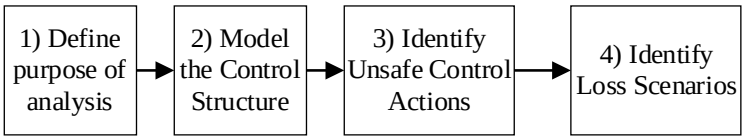

Figure 1. *STPA Process. (modified from* [5]*)*

The first step involves defining the purpose of the analysis, which is guided by sub-steps that include specifying losses, system-level hazards, and system-level constraints. In instances where a more detailed perspective is deemed beneficial, hazards and constraints may be optionally refined. Losses play a crucial role in steering the analysis, as they guide the focus of the STPA practitioner on specific hazards to investigate. In the context of STPA, hazards refer to the states a system can be in just before a loss might occur.

The second step, the modelling of the control structure, lays the groundwork for the actual hazard analysis. The control structure, exemplified in Figure 3, serves as a hierarchical representation of the system elements related to system control, encompassing components such as (human) controllers, sensors, and actuators. Commands, also called as *control actions* (CAs), are represented by downward arrows, and are transmitted from elements with higher hierarchical power to those with less. Feedback streams, represented by upward arrows, convey information to support controller decision-making. External inputs are depicted through horizontal arrows and must be included if their neglect otherwise leads to an incomplete representation of the system under investigation.

STPA gives special attention to CAs by dedicating Step 3 to identifying of how assumingly suitable and safe CAs can become unsafe. This step results in a list of UCAs, describing conditions that could lead to their realization. The analysis distinguishes between four types of UCAs: "Provided," "Not provided," "Provided, but at the wrong time" (too early, too late, or in the wrong order), and "Provided for an inappropriate duration" (for too long or too short).

Objective of STPA Step 4 is to examine all system elements like physical components, feedback, other inputs, and controllers for their potential to trigger UCAs, and give rise to losses. Moreover, since STPA Step 3, identifies UCAs without exploring how they translate into losses, Step 4 bridges this gap by examining the mechanisms through which also UCAs can manifest as actual losses. The result of this step, and the analysis as a whole, is a collection of textual descriptions referred to as loss scenarios. Essentially, these loss scenarios describe causal relationships among contributing factors, that can lead to the realization of one or more losses from step 1.

3 CASE STUDY

3.1 The mine automation system

The overall case system consists of an Automated Operating Zones (AOZ) including a surface drilling fleet which performs drilling activities on an open- pit mine. The fleet composes of three individual drill rigs which are operated either locally from within the cabin or remotely from a teleoperation station. Additionally, the drill rigs are capable of certain autonomous operations. The overall concept of automated and remotely operated drill rig fleet at an open-pit mine are presented in Figure 2.

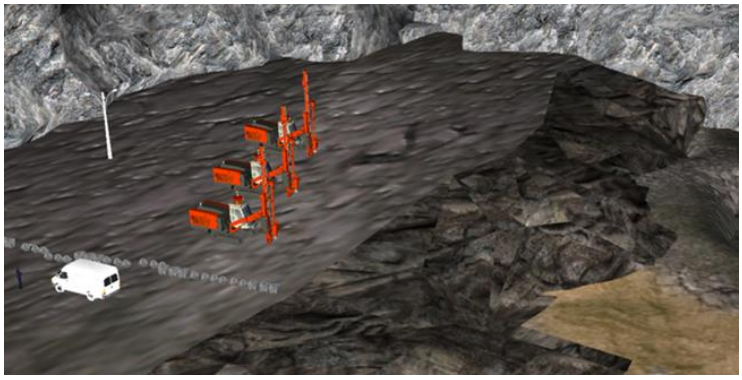

Figure 2. *The open-pit mine with three drill rigs.*

The use-case examined with STPA is part of a overall case system but narrowed down to maintenance operations performed to the three drill rigs on one AOZ. Reasons for maintaining drill rigs can be for example, the need to change a drill bit, a troubleshooting situation, or a planned service action. Maintenance work requires one or more maintenance persons to enter the AOZ and approach a drill rig which requires their attention. In our use-case this drill rig is currently remotely operated, meaning that maintenance operation must be planned first. To coordinate the maintenance operation either the maintenance person or the remote operator at the teleoperation station initiates communication with each other and requests maintenance. Upon this request the remote operator conducts a series

of steps to change the drill rig's operating mode from remote to local, as only local operation allows the maintenance worker to approach the drill rig safely. The maintenance worker can monitor the drill rig's operating mode and safety status through various signals, not only on the drill rig itself. These signals indicate whether it is safe to enter the AOZ or not. Once the maintenance work is concluded, the maintenance person leaves the drill rig and AOZ and informs the remote operator to take up the remote operation. Again, multiple steps need to be conducted by the maintenance person to indicate to the remote operator that it is safe to switch from local to remote operation. Another factor, which this use-case considers is, that maintenance persons are not restricted to pair work and if required can simultaneously and individually work on one drill rig. Consequently, each drill rig is equipped with safety system components to indicate its operating mode to other maintenance persons on the AOZ.

3.2 Application of STPA on mine automation system

3.2.1 STPA Step 1

The purpose of this analysis is summarized in Table 1. The higher-level losses, so called system-level losses, to be prevented are loss of human life and any object part of the operation as well as threats to the mission. System-level hazards must be prevented as they may result in these specified losses, for example when a drill rig or its actuators move when people are nearby. Visualized with square brackets ([ ]), each system-level constraint addresses a respective hazard and specifies on a higher level how to prevent these undesirable system states.

Table 1. *Purpose of analysis.*

System-level Losses	System-level Hazards	System-level Constraints
L-1 Loss of life or injuries to humans	H-1 Drill rig drives when people are nearby [L-1], [L-4]	SC-1 Drill rig may not drive when there are people nearby. [H-1]
L-2 Loss of or damage to vehicle (drill rig or others)	H-2 Drill rig moves when vehicles or other objects are in its way [L-2][L-3][L-4]	SC-2 Drill rig must stop when there are vehicles or other objects in the way. [H-2]
L-3 Loss of or damage to objects outside the drill rig	H-3 Drill rig actuators activate when people are nearby. [L-1][L-4]	SC-3 Drill rig actuators may not activate when there are people nearby. [H-3]
L-4 Loss of mission (drilling operation)	H-4: Drill rig leaves the area where it is intended to operate. [L-1][L-2][L-3][L-4]	SC-4 Drill rig must stay in the area where it is intended to operate. [H-4]
	H-5: Drill rig stops operating unintentionally. [L-4]	

3.2.2 STPA Step 2

The final hierarchical control structure went through several refinement iterations using MS Visio. However, for confidentiality reasons, only an extract can be viewed in Figure 3. Colour coding is employed to emphasize distinct system elements. The CAs relevant to this analysis are numbered and highlighted in red. Despite not directly relevant to this analysis, other CAs and feedback streams are listed to increase the reader's understanding of the use-case and control structure. Textual descriptions of the system's operation in various modes served as primary source of information. Conversations with system experts guaranteed a hierarchically accurate representation of the use case.

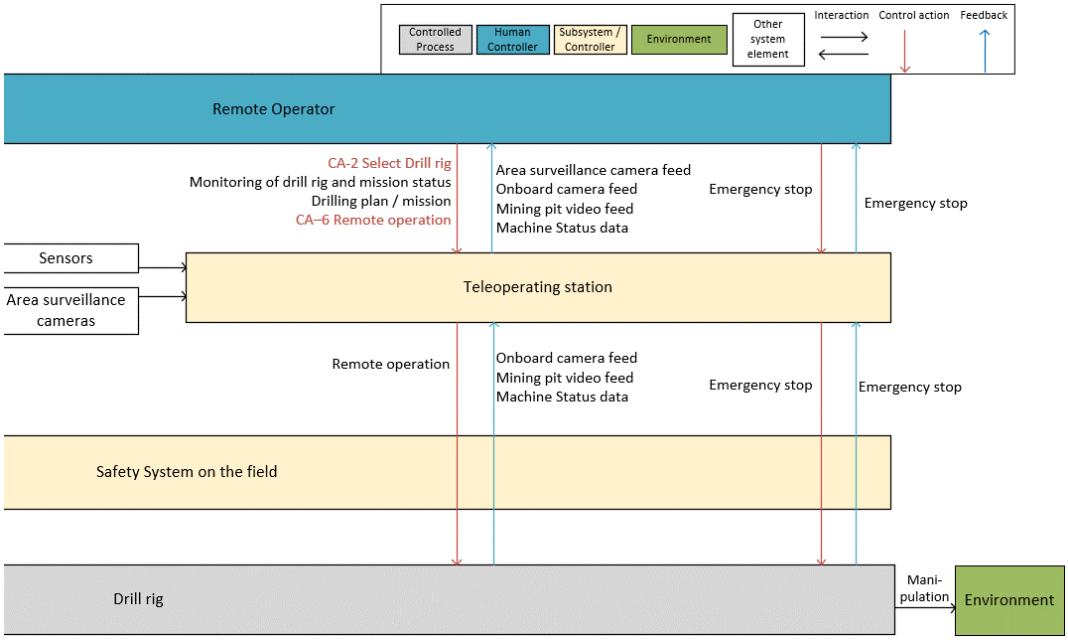

Figure 3. *Extract of highly abstract, hierarchical control structure.*

3.2.3 STPA Step 3

In step 3, the following CAs were analysed (in red on Figure 3.):

- CA-1 Communication via mobile phone / radio
- CA-2 Drill rig selection
- CA-3 Drill rig operating mode selection (Local/Remote)
- CA-4 Acknowledgement of Teleoperation selection (transmitted from maintenance person to Safety system on field)
- CA-5 Setting the drill rig back to remote operation mode (transmitted from Safety system on field to drill rig)
- CA-6 Remote operation (transmitted from Remote operator to teleoperating station)

Key considerations when defining the context in which a CA could develop into an UCA were the different operating modes the drill rig can enter (local operation, remote operation), the necessary procedures to be performed by remote operators and maintenance personnel as well as the indications of operating modes and states of transition.

Altogether 15 UCAs were identified originating from the 6 CAs. As an example, CA-1 turning into UCAs based on the four types can be viewed in Table 2:

Table 2. *UCAs that originate from CA-1.*

Provided	**Not provided**
UCA-1.1 Operator 1 provides wrong information about which drill rig parts need to be maintained. [H-1] [H-3] [H-5] UCA-1.2 Operator 1 provides wrong location/name of drill rig to maintenance person. [H-1] [H-3] [H-5]	UCA-1.3 Operator 1 does not communicate to Maintenance person, that drill rig needs to be maintained [H-5]
Provided too soon / too late / in wrong order	**Stopped too soon / applying too long**
UCA-1.4 Operator 1 communicates too late to Maintenance person, that drill rig needs to be maintained [H-5]	N/A

3.2.4 STPA Step 4

Step 4 results in the main findings of the analysis, the list of loss scenarios. This list is retrieved by brainstorming various combinations of worst-case factors. For our use-case 48 loss scenarios were identified out of which 31 originate from UCAs. Other loss scenarios originate from feedback streams and system elements themselves.

Below, each one exemplary loss scenario originating from an UCA, a feedback stream and a system element is given (Table 3). The table groups related loss scenarios together for clarity, as seen for loss scenario-1 and -20.

Table 3. *Exemplary set of loss scenarios.*

Loss Scenario	Scenario Description	Related UCA / Feedback / System element
Loss Scenario-1	Maintenance person follows operator's instructions and approaches the drill rig without checking the operating mode indicator. This can cause the drill rig to move when the maintenance person is in its vicinity [H-1] [H-3]. This can happen because: - Operator 1 himself receives wrong information about which drill rig parts need maintenance. - Operator 1 confuses the drill rig parts when informing the maintenance worker. - Operator 1 sends incomplete message due to poor connection.	UCA-1.1
Loss Scenario-10	Maintenance person sends incomplete message due to poor connection. This could cause delay in production [H-5] and depending what situation the maintenance worker is facing, poor or no communication could risk his or others health. [H-2]	Feedback-1 Communication (Maintenance person to Operator 1)
Loss Scenario-20	Maintenance person wants to speed up the process and already starts moving towards the drill rig without waiting for the information from the operating mode indicator. [H-1] Maintenance person believes the operating mode indicator will give information any moment and starts moving towards the drill rig [H-1] [H-3].	Maintenance person (human, system element)

Most loss scenarios were identified due to human-machine interactions, followed by loss scenarios due to human-human interactions and machine / engineering types of problems. Engineering type of problems include for example failure in power supply of radio or malfunction of the operating mode indicator in the drill rig. Also, loss scenarios based on misunderstandings between the remote operator and the on-site maintenance personnel as well as between the on-site maintenance personnel are critical. Most relevant loss scenarios arise from on-site maintenance personnel facing challenges related to the indication of the operating mode of the drill rig and its transitions. Additionally, the choice of location of on-site control cabinet and consequently its visibility affects safety.

4 DISCUSSION

The loss scenarios indicate the critical nature of communication between maintenance workers and remote operators. Consequently, it becomes imperative to prevent connectivity issues arising from phone or radio malfunctions. Moreover, STPA revealed that the operation greatly depends on the functionality of the operating mode indicator and maintenance personnel strictly following instructions and not forgetting to check or misinterpreting the operating mode indicator when approaching the drill rig. Therefore, we propose clear operating mode indication, good site overview and visibility to prevent unintended drill rig approaches during drill rig's automatic operation. Based on these findings, we argue that STPA provides valuable insights into possible hazards arising from this use-case's maintenance operation and consequent drill rigs' operation mode changes.

Compared to other STPA analyses ([8]), the 15 UCAs and almost 50 loss scenarios are relatively limited in quantity. This may be attributed to the narrowly defined use-case and the restriction to analysing only six control actions. A significant share of loss scenarios is related to human-machine and human-human interactions. Therefore, leveraging available methodologies for examining human behaviour ([9]) could have possibly led to an even higher amount and more detailed loss scenarios.

Not only the official output of the STPA process – the collection of loss scenarios – yields insights to possible safety risks within the system under investigation. Also, the results from steps 2 and 3—the hierarchical control structure and the list of UCAs—, which support the creation of loss scenarios, provide crucial information which shall not be underestimated. Further research could investigate how the hierarchical control structure can support also other system and safety engineering activities.

Furthermore, the loss scenarios in their current representations are merely descriptions of combinations of worst-case factors resulting in loss and do not directly support system designers and decision makers in formulating system design and safety requirements. We argue, that STPA could be even more useful if its output would be in a format that supports decision makers in defining requirement specifications.

5 CONCLUSION

We see STPA as a relevant complementation to other safety analysis tools as it leads to noteworthy findings that support the design and evaluation of automated mining operations. STPA gives valuable insights as it views safety as a control problem and considers effects within and to the whole system process. While the results are not of technical nature, they can aid in creating a safe work environment and understanding factors affecting the work at the site. STPA proved to deliver valuable input for discussions during system's conceptual design phase. Additionally, the tool appears to contribute to assessing planed system design modifications as well as reassessing already existing systems. We suggest further research on STPA, particularly focusing on improving its usability for formulating concrete safety requirements and validation criteria regarding sensing and detection capabilities, safety functionalities, communication solutions.

6 ACKNOWLEDGEMENT

This paper is related to the work done in VTT in the Business Finland funded "FEMMa" research project in its task 4.2 "System-theoretic approach for the identification of autonomy and electrification related risks".

7 REFERENCES

[1] A. Hentunen *et al.*, "Future Electrified Mobile Machines 'FEMMa' Elinkeinoelämän kanssa verkottunut tutkimus."

[2] T. Fu, T. Zhang, Y. Lv, X. Song, G. Li, and H. Yue, "Digital twin-based excavation trajectory generation of Uncrewed excavators for autonomous mining," *Autom Constr*, vol. 151, Jul. 2023, doi: 10.1016/j.autcon.2023.104855.

[3] S. Ge *et al.*, "The Use of Intelligent Vehicles and Artificial Intelligence in Mining Operations: Ethics, Responsibility, and Sustainability," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1021–1024, Feb. 2023, doi: 10.1109/TIV.2023.3246118.

[4] S. Baumgart, J. Froberg, and S. Punnekkat, "Can STPA be used for a System-of-Systems? Experiences from an Automated Quarry Site," in *2018 IEEE International Systems Engineering Symposium (ISSE)*, 2018, pp. 1–8.

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

[6] N. Leveson, *Engineering a Safer World*. Massachusetts Institute of Technology, 2011.

[7] N. Leveson, "A new accident model for engineering safer systems," 2004, doi: 10.1016/S0925-7535(03)00047-X.

[8] H. Kim, M. A. Lundteigen, A. Hafver, and F. B. Pedersen, "Utilization of risk priority number to systems-theoretic process analysis: A practical solution to manage a large number of unsafe control actions and loss scenarios," *Proc Inst Mech Eng O J Risk Reliab*, vol. 235, no. 1, pp. 92–107, Feb. 2021, doi: 10.1177/1748006X20939717.

[9] M. E. France, "Engineering for Humans: A New Extension to STPA," Master's Thesis, Massachusetts Institute of Technology, 2017. Accessed: Dec. 04, 2023. [Online]. Available: http://hdl.handle.net/1721.1/112357