THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Human-system integration risk assessment for automation in mining

AProf Maureen Hassall, School of Chemical Engineering, UQ

Dr Ben Seligmann, Minerals Industry Safety and Health Centre, UQ

Prof Robin Burgess-Limerick, Minerals Industry Safety and Health Centre, UQ

Dr. Danellie Lynas, Minerals Industry Safety and Health Centre, UQ

Prof Joel Haight, Swanson School of Engineering, The University of Pittsburgh

Human-system integration risk assessment for automation in mining

Abstract

The objective of the project was to answer the question: What risk assessment techniques deliver the most effective and user accepted means of identifying risks associated with human-system interactions in remote-controlled and autonomous mining operations?

Four hazard identification methods were assessed across three case studies – human-autonomous surface haulage interactions, autonomous longwall mining and remote control of processing plants:

1. Preliminary Hazard Analysis (PHA/HAZID) (Traditional Method)
2. Failure Mode and Effects Criticality Analysis (FMECA) (Traditional Method)
3. System Theoretic Process Analysis (STPA) (Systems-theory Method)
4. Strategies Analysis for Enhancing Resilience (SAfER) (Systems-theory Method)

The methods included a literature review, an analysis of the outcomes of workshops with industry participants, and a survey of participants' feedback. Three one-day workshops were held in a combination of face-to-face and remote modes with 8-9 industry participants in each.

Feedback from the participants and analysis of workshop information suggest that no single approach is effective alone across the range of automation case studies. Using multiple methods may well be advantageous. HAZID is easy to use, and perceived as most useful for identifying threats. SAfER was perceived as the most effective for identifying magnitude of impacts and suggesting follow-up actions. SAfER also had the highest overall effectiveness. HAZID is useful for broader scopes and lower required detail, whereas FMECA, STPA and SAfER are naturally narrower in scope but can support a more detailed focus analysis in a particular area: equipment failure, control system design holes and human decision strategies. A combination of different methods could be the best way forward, however it may be that only parts of each method need to be combined with parts of another, rather that perform two or more full analyses.

Further work should be done to investigate a hybrid approach. Such an approach might consist of:

1. Setting the scope including a human-system interaction diagram (as was produced in STPA).
2. HAZID (for existing systems) or STPA based FMECA (for new systems)
3. Combining the technique from 2. with refined version of SAfER to identify risks and control options.

The STPA based FMECA could comprise the following:

1. Identify the control action from the human-system interaction diagram. Determine relevant failures (including those suggested by STPA).
2. Identify possible causes of the failures
3. Identify possible effects of the failures
4. Assess the effects using the impacts ratings from the risk matrix
5. Assess the likelihood and determine risk rank
6. Recommendations for improving design and/or adding layers of protection (controls) to address those interactions with unacceptable levels of inherent risk.

The refined version of the SAfER process should involve referencing the human-system interaction diagram, performing the situation assessment analysis with the addition of a risk ranking if indicator was absent/overlooked and/or incorrect/misleading. The identification of causes and consequences of strategies along with a risk ranking of them should also be added to the SAfER table.

1. Table of Contents

2. Introduction:

The mining industry is developing and implementing automation and other new technologies at an increasing rapid rate. Examples include autonomous haul trucks, autonomous drills, automated longwall miners, remotely operated processing plants, autonomous trains and smaller robots and drones. Such technologies are adopted to improve worker health and safety by reducing their exposure to high risk situations, as well as to improve operational efficiencies. However, automation and the adoption of new technologies does not completely remove people from operations. Technology still needs to be cleaned, serviced and maintained by humans. Thus, the introduction of autonomous and automated technologies has the potential to introduce new and different human-system interaction risks. Such risks are evident in the following accidents:

- The 2015 collision between an autonomous haul truck and manned water cart that resulted in significant damage to the truck and minor injuries to the water cart driver – refer to https://www.dmp.wa.gov.au/Documents/Safety/MS_SIR_226_Collision_between_an_autonomous_haul_truck_and_manned_water_cart.pdf for more details.
- The 2015 death of a worker after being stabbed/shocked by a welding robot – refer to https://www.emirates247.com/business/technology/robot-kills-co-worker-in-a-car-factory-in-india-2015-08-14-1.600317 for more details.
- The 2017 fatal crushing of an underground coal mining worker by a remote controlled continuous cutting machine – refer to https://www.msha.gov/data-reports/fatality-reports/2017/fatality-8-june-13-2017/final-report for more details.
- The 2019 automated train accident that injured more than a dozen people when the driverless train incorrectly travelled in the wrong direction – refer to https://www3.nhk.or.jp/nhkworld/en/news/backstories/569/ for more details

Previous major industrial incidents have shone the spotlight on deficiencies in current risk assessment and risk treatment practices. Examples include:

- The 2010 Pike River mine explosion in which 29 people were killed. It was the Royal "commission's view that even though the company was operating in a known high-hazard industry . . . and the **executive managers did not properly assess the health and safety risks that the workers were facing**. . . and exposed the company's workers to unacceptable risks." (Royal Commission Report 2012 p. 12)
- The 2014 Hazelwood mine fire that burned for 45 days and resulted in a town being evacuated and residents experiencing short and long term health issues. The Inquiry into the fire found that the "**fire was a foreseeable risk that slipped through the cracks . . . This reality must be confronted if similar incidents are to be avoided in the futur**e" (Hazelwood Mine Fire Inquiry Report, 2014 p. 18)
- The 2018 Uber crashed which killed a pedestrian was, according to the NSTB caused by The failure of the vehicle operator to monitor the driving environment and the operation of the automated driving system" and Uber's "**inadequate safety risk assessment procedures . . . ineffective oversight of vehicle operators, and lack of adequate mechanisms for addressing operators' automation complacency**" (NTSB *report)*

The risk assessment process is outlined ISO31000:2018 the International Standard for Risk Management as shown in the green box of Figure 1. When risk assessments are undertaken for mining and related operations, they often done so using traditional hazard identification techniques.

Figure 1: Risk management process as described in ISO31000

Such techniques are referred to as Hazard Identification techniques (HAZID), Broad Brush Risk Assessments (BBRA), Process or Job Hazard Analysis (PHA or JHA), Failure Mode and Effects Analysis or Failure Modes and Effects Criticality Analysis (FMEA or FMECA) or similar. These techniques were developed decades ago and have not been designed to capture the novel and emergent hazards associated with the introduction of new technology, nor with dysfunctional interactions can occur in software-enabled, socio-technical systems where accidents happen even though no individual component failed (Dekker, Cilliers, & Hofmeyr, 2011). Some research has found that traditional risk identification (HAZID) have been shown not to be effective for software-enabled technologies embedded within socio-technical systems (Leveson, 2012).

New socio-technical risk assessment approaches such as System Theoretic Process Analysis (STPA) and Strategies Analysis for Enhancing Resilience (SAfER) have been developed and tested to identify risks associated with the introduction and control of technologies in complex socio-technical system, with promising results. However, such techniques have not been tested on mining applications nor with mining industry practitioners. To address this gap, research was conducted with mining industry personnel, to test and assess the efficacy of different risk assessment techniques in identifying human-system interaction risks associated with monitoring, maintaining and controlling autonomous and semi-autonomous systems in mining contexts.

3. Purpose:

The research sought to answer the following research question:

> **What combination of risk assessment techniques delivers the most effective means of identifying risks associated with human-system interactions in remote and autonomous mining operations?**

This question will be answered by conducting a comparative study, where the following four HAZID methods will be investigated:

1. Preliminary Hazard Analysis (PHA) (Traditional Method)
2. Failure Mode and Effects Criticality Analysis (FMECA) (Traditional Method)
3. System Theoretic Process Analysis (STPA) (Systems-theory Method)
4. Strategies Analysis for Enhancing Resilience (SAfER) (Systems-theory Method)

The investigations will include a formal literature review as well as collaborative workshops with industry personnel to test and assess the application of these techniques on the following three case studies:

1. Human-system interactions in surface mine automated haulage areas
2. Autonomous longwall mining operations underground
3. Remote control of coal processing plants

Specifically the objectives associated with the industry personnel collaborations are:

- Familarisation training in the preparation and application of the techniques
- Conducting collaborative workshops to apply the techniques to produce HAZID, FMEA, SAfER and STPA analyses on abovementioned case studies
- Evaluating the outputs of the techniques in terms of the identification of technical, human and human-technical interaction risks associated with the supervision and control of autonomous haulage technology.
- Collecting industry participant feedback on the usability and usefulness of each technique in delivering meaningful insights into human-system interaction risks associated with automated haulage and semi-autonomous operations.

It is important to note that the risk assessments produced were based on a hypothetical and generalised scope. They did not relate to a specific context or technology and therefore should not be considered or used as an actual operations' risk assessment. Operations considering or actually introducing or operating autonomous or semi-autonomous machines must undertake their own risk assessments.

4. Method:

A tripartite approach was taken to the methodology as shown in Figure 2. The detailed method for each of the three pieces of research is described next.

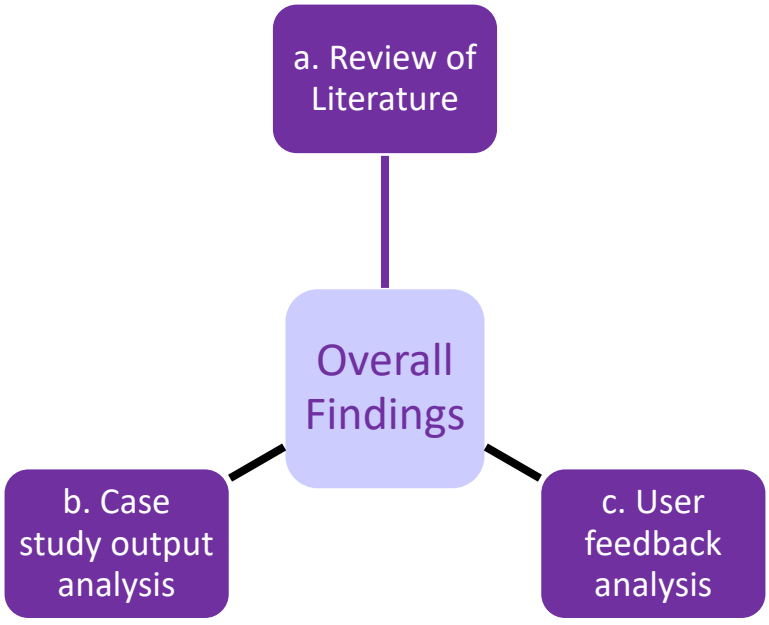


Figure 2: Overall research approach

a. Literature review

A literature search was conducted by exploring the history and the application of the hazard analysis and risk assessment methodologies used in industries around the world other than in the mining industry. The research body of knowledge in terms of comparing methods for effectiveness is lean and so branching into other industry sectors was necessary. Also included were articles about application and actual practice in industry since the research was lean. The anecdotal practices and how and how often the methods are used was included as that also indicates what methods people prefer.

Data bases searched:

ScienceDirect
Scopus
Web of Science

Key words used included HAZOP, FTA, What If, FMEA, STPA, STAMP, SAfER, PRA, QRA, hazard, safety, Risk and Risk Assessment. As a result, over 600 papers were screened with only 20 remaining for inclusion.

b. Case Study Analysis

As mentioned above the case study analysis investigated studied:

- Surface mine automated haulage;
- Underground longwall automation; and
- Remote processing plant operation scenarios.

The purpose of performing risk assessments on these case studies was to:

- Identify human-system interaction risks associated with the supervision and control of autonomous haulage technology
- Use the identified human-system interaction risks to assess the efficacy (in terms of usability and utility) of different risk assessment techniques

To perform the risk assessments on each of the case studies, this project undertook the following:

1. Representatives from industry were invited to participate in different case study analyses.
2. In collaboration with industry participants, a scope was developed for the three case study scenarios prior to the workshop which outlined the scenario using diagrams and with a scope table that used the PLEATS framework described in Table 1.

Table 1: Outline of scope table used in risk assessment

Attribute of scope	Included	Excluded
P: People involved in risk management or potential impacted if risks are not managed		
L: Locations or areas where the risk exist or that could be impacted if the risk event materialised		
E: Equipment and plant (e.g. tools, vehicles, fixed processing plant, infrastructure etc)		
A: Activities (e.g. operations, maintenance, startups etc)		
T: Timeframe (e.g. present time and how far into the future)		

S: Known risk scenarios that need to considered		

3. Preparation for workshop by developing workshop slides for four risk assessment techniques: HAZID, FMECA, SAfER and STPA
4. A separate one day workshop was conducted for each case study using the scope developed (in step 2) and slides prepared (in step 3) and by following the agenda that covered:

8:00am	Introductions, confirm scope and brief overview of techniques
8:45am	Introduction and application of first technique - HAZID
10:00am	Group debriefs of HAZID technique
10:15am	Introduction and application of second technique – FME[C]A
11:30am	Group debriefs FME[C]A technique
11:45am	Break
12:45pm	Introduction and application of third technique - SAfER
2:00pm	Group debriefs SAfER technique
2:15pm	Introduction and application of fourth technique - STPA
3:30pm	Group debriefs STPA technique
3:45pm	Debrief day
4:00pm	Close

5. For the application of each technique an Excel workbook.
    a. The HAZID process that was followed in each case study is shown in Figure 3 and the example workbook shown in Figure 4.
    b. The FMECA spreadsheet is shown in Figure 5 and the FMECA process shown in Figure 6.
    c. The SAfER process that was followed is highlighted in Figure 7 and documented on the spreadsheet in Figure 8.
    d. STPA process was taken from Leveson & Thomson 2019 retrieved from http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf which is shown in Figure 9. The spreadsheet used is shown in Figure 10.

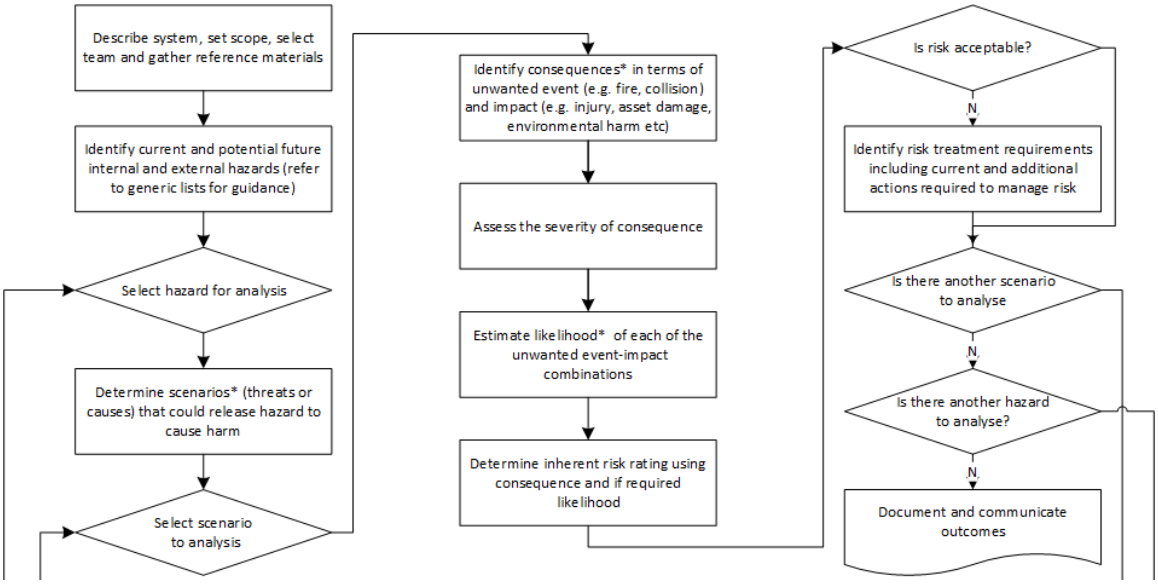


Figure 3: Process flow diagram for HAZID process

Project Name: EU Workshop on Autonomous Longwall Mining

Scope: Refer to scope document

Insert the IMPACT Number from the RAM under People, Assets, Environment, Reputation

Insert the most appropriate descriptor for LIKELIHOOD from the RAM

Description of Hazard	Description of unwanted event scenarios	Causes	Consequences	Potential Impact					Risk analysis		Risk evaluation and recommendations on risk treatment options (i.e. in terms of Inherently Safer Design and Defence in Depth/Hierarchy of Controls)	What controls are required to effectively manage the risk	What monitoring and review is required to ensure the risks and risk controls are effectively managed	Responsible person
				People	Assets	Environment	Reputation	Max Impact	Est Likehood	Overall Risk Rank				

Figure 4: Outline of HAZID workbook

Failure Modes Effects Criticality Analysis

Project Name:

Scope:

Insert the IMPACT Number from the RAM under People, Assets, Environment, Reputation

Insert the most appropriate descriptor for LIKELIHOOD from the RAM

Component Name	Component Function	Failure Mode(s)	Cause(s) Of Failure	Effect(s) Of Failure	Potential Impact					Risk analysis		Risk evaluation and recommendations on risk treatment options (i.e. in terms of Inherently Safer Design and Defence in Depth/Hierarchy of Controls)	What controls are required to effectively manage the risk	What monitoring and review is required to ensure the risks and risk controls are effectively managed	Responsible person
					People	Assets	Environment	Reputation	Max Impact	Est Likehood	Overall Risk Rank				

Figure 5: Outline of the FME[C]A process

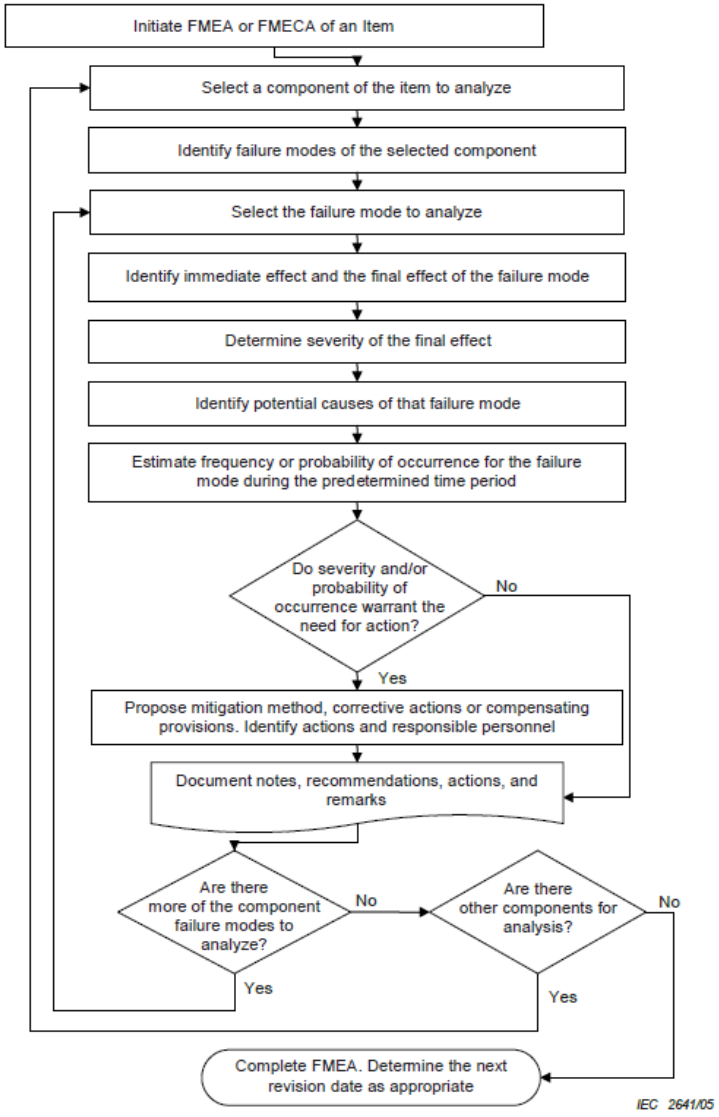
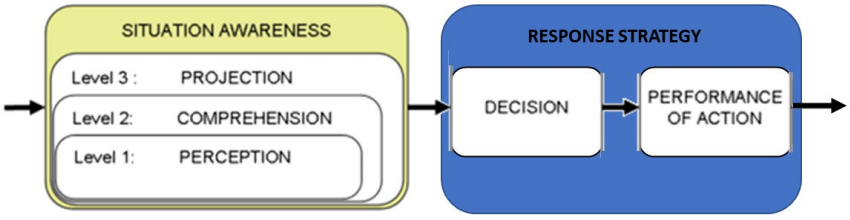


Figure 6: FMECA process as outlined in IEC60812



STEP 1:
Identify the indicators of safe/unsafe operations factors and ensure the design makes them OBVIOUS so that they are

- Very easy to perceive
- Very easy to comprehend
- Very easy to project

STEP 2:
Identify the range of ways people can perform work in normal and abnormal situations using generic strategy prompts then identify design changes that can help operators produce successful outcomes across a range of situations by:

- Helping them make the right decisions in terms of strategy selection
- Having a user-friendly design so the performance of actions can be done efficiently and effectively

Figure 7:SAfER process

Situation Assessment Indicators	List the indicators that need to be monitored to check for safe/unsafe operation?		What design improvements could make these indicates easy to perceive, comprehend and project into the future?	
Plant/process factors				
People factors				
Context factors				
Generic Strategy Prompts	**What plausible decision/actions related to this generic strategy could be used in the system being analysed?** (Consider examples for both normal and abnormal operations)	**What consequences might result if people adopt this strategy?**	**Should design promote, prevent or tolerate strategy?**	**What design improvements would improve response strategies during normal, abnormal and unexpected situaitons?**
Avoidance = Not done, defer, or forget to do				
Intuitive = automatic response, done without explicitly or deliberately using thought processes				
Arbitrary-choice = guessed, scrambled haphazard or panicked response				
Imitation strategies = copy how others do it or copy what has worked in the past				
Cue-based strategies = select Chosen Option using the Observed Info/Cues and Predict Consequences results				
Compliance-based strategies = following procedures as they are written/practiced				
Analytical Reasoning strategies = using analytical thinking to reason out the best way to perform task				

Figure 8: SAfER Spreadsheet

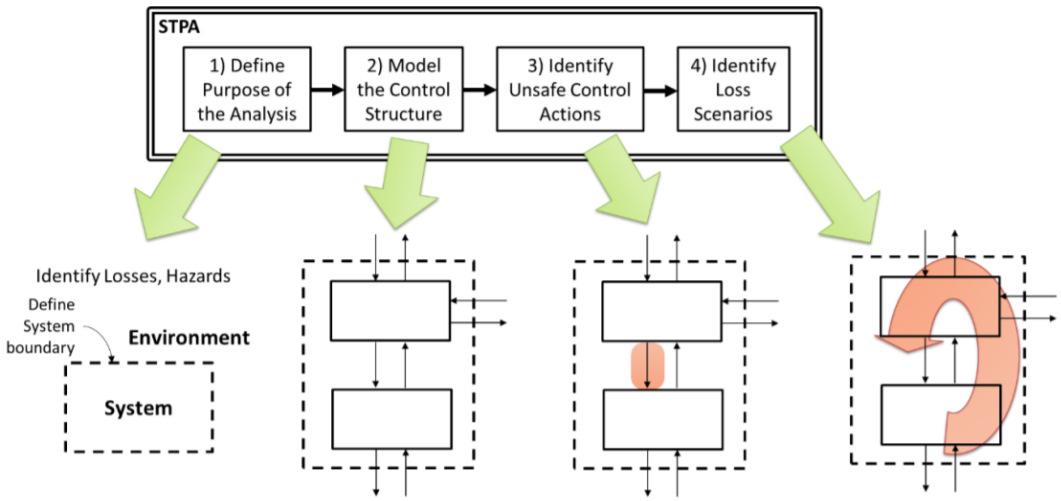


Figure 9:STPA process (from Leveson & Thomson 2019)

Systems Theoretic Process Analysis (STPA)

Project Name: _____

Control action	Control Action NOT GIVEN	INCORRECT Control Action IS GIVEN	Control Action GIVEN AT WRONG TIME - TOO SOON/EARLY	Control Action GIVEN AT WRONG TIME - TOO LATE	Control Action GIVEN IN WRONG ORDER or FOR WRONG DURATION	Potential Consequence(s) and Significance (High priority - must address, Med priority - should address, Low priority - monitor for change, Negligable - No further action required)	Possible causes of unsafe control action	Assessment and recommendation for improving design (ISD) or controls or control systems (DiD)

Figure 10: STPA spreadsheet

6. After the workshops the output from each technique was finalised, analysed and compared across the techniques.
7. The findings from the technique analysis (step 6) were then compared with the literature review and user feedback findings to elicit further insights.

c. User feedback analysis

1. Ethics approval was obtained to collect survey information, conduct interviews and collect other information (e.g. incident investigation data and reports) in a manner that allows for it to be published.
2. Surveys were conducted to capture baseline knowledge and the practitioners' perspectives on strengths, weaknesses, opportunities and threats associated with:
   - current and future human-automation interaction risks
   - the efficacy (useability, usefulness and effectiveness) of current risk techniques in identifying, assess and action potential upside and downside risks. A copy of the surveys are attached in Appendix A
3. During the workshop and after trailing the application of each technique, further survey questions were asked that allowed individuals to provide their feedback on each technique in

terms of its understandability, ease of use, usefulness in producing quality outcomes and any other comments.

4. Analysis process:

The survey results for every question, both pre and post workshop were extracted from Survey Monkey, or from the paper-based surveys, and collated in Excel. Then graphs for the answers to each question were created.

The survey results for the Haulage workshop were only available for pre-workshop surveys. The post-workshop surveys were not collected, although the reason for this is uncertain.

a. 1.1 Metrics applied

A measure of the 'mean' of the distributions for each graph was calculated, for questions 4-7 of the pre-workshop survey and 1-4 of the post-workshop survey. We can consider the y-axis to be a qualitative representation of a continuous variable: either "ease of learning" or "effectiveness". By representing, for example, 'very ineffective' with a value of 1, and 'very effective' with a value of 5, a mean for each methods' distribution can be calculated; for example, see Figure A18. These mean values were used to compare:

- Answers to questions 4-7 of pre-workshop survey's for the three different groups of participants, to understand any pre-existing differences between the groups.
- Pre-and post-workshop perceptions of participants in each workshop, for each question asked.
- Post-workshop answers applicable to each method, to compare the perceptions of participants regarding each method used.

The second metric that was applied to the answer distributions is the Shannon Entropy Ratio (SER). The Shannon Entropy is a measure of information related to the distribution. The Shannon Entropy is maximized when the distribution is a uniform distribution, and it is minimized (at a value of 0) when all data points have the same value. These two extremes represent either 'knowing' nothing about the variable - i.e. if a uniform distribution, the actual value could sit anywhere in the distribution – or being completely sure of the value – i.e. the situation where all data points have the same value.

The Shannon Entropy is used as a measure of *how much consensus* the relevant group of participants had for the particular method they were addressing in each survey question. This is analogous to a measure of the spread of data points around the mean, but it is distinct from the standard deviation. Using the Shannon Entropy measures the spread, but in particular it indicates the amount of information known/unknown about that distribution – thus an indication of consensus. For example, a uniform distribution with the same standard deviation and mean as a gaussian distribution don't have the same information content – there is less certainty about the uniform than the gaussian. This can be directly related to an indication of the consensus of a group of people, and thus the Shannon Entropy was selected as a metric for this analysis.

The Shannon Entropy Ratio is simply the ratio of the Shannon Entropy of the distribution divided by the Shannon Entropy of a uniform distribution over the 5 categories of very ineffective/hard -> very effective/easy. This gives a percentage of how close to the uniform distribution the answer distribution is. This is an easy and clear way to compare the level of consensus for each answer distribution. The value of the SER ranges between 0 and 1.

The Shannon Entropy is calculated using Equation 1.

Equation 1 - Shannon Entropy (SE)

$$SE = -\sum_{i=1}^{n} P_i \ln(P_i)$$

Where n is the number of categories (5 levels from very ineffective/hard -> very effective/easy), and P is the probability of the variable (e.g. 'How easy to learn") is in each category. To calculate the Shannon Entropy Ratio (SER), the SE of a uniform distribution with 5 categories (uniform distribution would give a probability of 20% for each of the 5 categories) for the values should be calculated, using Equation 2.

Equation 2 - Shannon Entropy of a Uniform Distribution of 5 levels

$$SE_{max} = -\ln(0.2)$$

Therefore, the SER is calculated by Equation 3.

Equation 3 - Shannon Entropy Ratio (SER)

$$SER = \frac{SE}{SE_{max}} = \frac{\sum_{i=1}^{n} P_i \ln(P_i)}{\ln(0.2)}$$

Since SER is calculated with reference to a uniform distribution of 5 levels, if a data set has less than 5 points, the SER may not be a very accurate measure of consensus. This is because it is not possible for a data set of less than 5 points to potentially fill the 5 levels of the distribution, and so the SER will overestimate the level of consensus for that question.

5. Results:

The results from each aspect of this research – the literature review, the workshops teaching and applying the different risk assessment techniques and the surveys collecting participant perceptions of each technique are described in the following subsections.

b. Literature review

The results of the literature review show that while some of the more systems-based and human factors-based methods are becoming more popular, the comparisons between traditional methods and the more modern approaches such as STPA, SAfER, and STAMP show that results are quite equivocal. While the traditional methods are better for some applications, the modern methods provide advantages for other applications. The method of choice seems to best determined by choice (ease of use, experience, level of satisfaction experienced), application, complexity of the system and by the specific application for the technique. Overall, it seems that the research shows that the use of the modern methodologies for hazard identification and risk assessment of automated systems fits well due to the need to consider human interactions (SAfER) and the need to evaluate an automated system using a systems-based approach (STPA).

c. Case study analysis

The automated surface haulage workshop was held as a virtual and in-person workshop on May 25, 2021. Nine industry participants and four researchers attended. The autonomous surface haulage case study including scope and workshop spreadsheets for HAZID, FMECA, SAfER and STPA is documented in Appendix B.

The automated longwall workshop was held as a virtually (due to COVID-19 restrictions) on August 2, 2021. Eight industry attendees and four researchers were present. The automated longwall mining case study including scope and workshop spreadsheets for HAZID, FMECA, SAfER and STPA is documented in Appendix C.

The remote controlled coal preparation plant workshop was held as a virtual and in-person workshop on August 23, 2021. Nine industry attendees and four researchers were. The automated longwall mining case study including scope and workshop spreadsheets for HAZID, FMECA, SAfER and STPA is documented in Appendix D.

Each workshop was able to complete each technique. Each process identified similar information. From workshop facilitation observations and an analysis of the outputs, the following observations were drawn:

- The HAZID process seemed to be familiar to the attendees, perhaps because similar risk assessment techniques are used in mining (although they may be called different things like WRAC, BBRA etc).
- The FMECA process was a bit more challenging to focus it on human-system interactions rather than on the equipment automation. Better understanding of the component function (e.g. the function of the human-system interaction) should help improve the efficacy of the technique.
- The SAfER technique new insights around situation awareness requirements and strategy options. The approach was new to participants so it took more effort and time to elicit information and a complete analysis was not produced from any of the workshops.
- The control diagram produced by the STPA also seemed to be a new process for participants it took some time to develop but it helped identify and clarify interactions. The resultant diagram made the analysis of deviations in human-system interactions reasonably straight forward.

d. Survey analysis of participants' perceptions.

Overall, participants found the HAZID process familiar and easy to use. However, comments were made that effectively outcomes relies on knowledgeable people understanding historical events in a given system which can make it challenging to apply HAZID to new systems. Results from the survey on HAZID are shown in Figure 11.

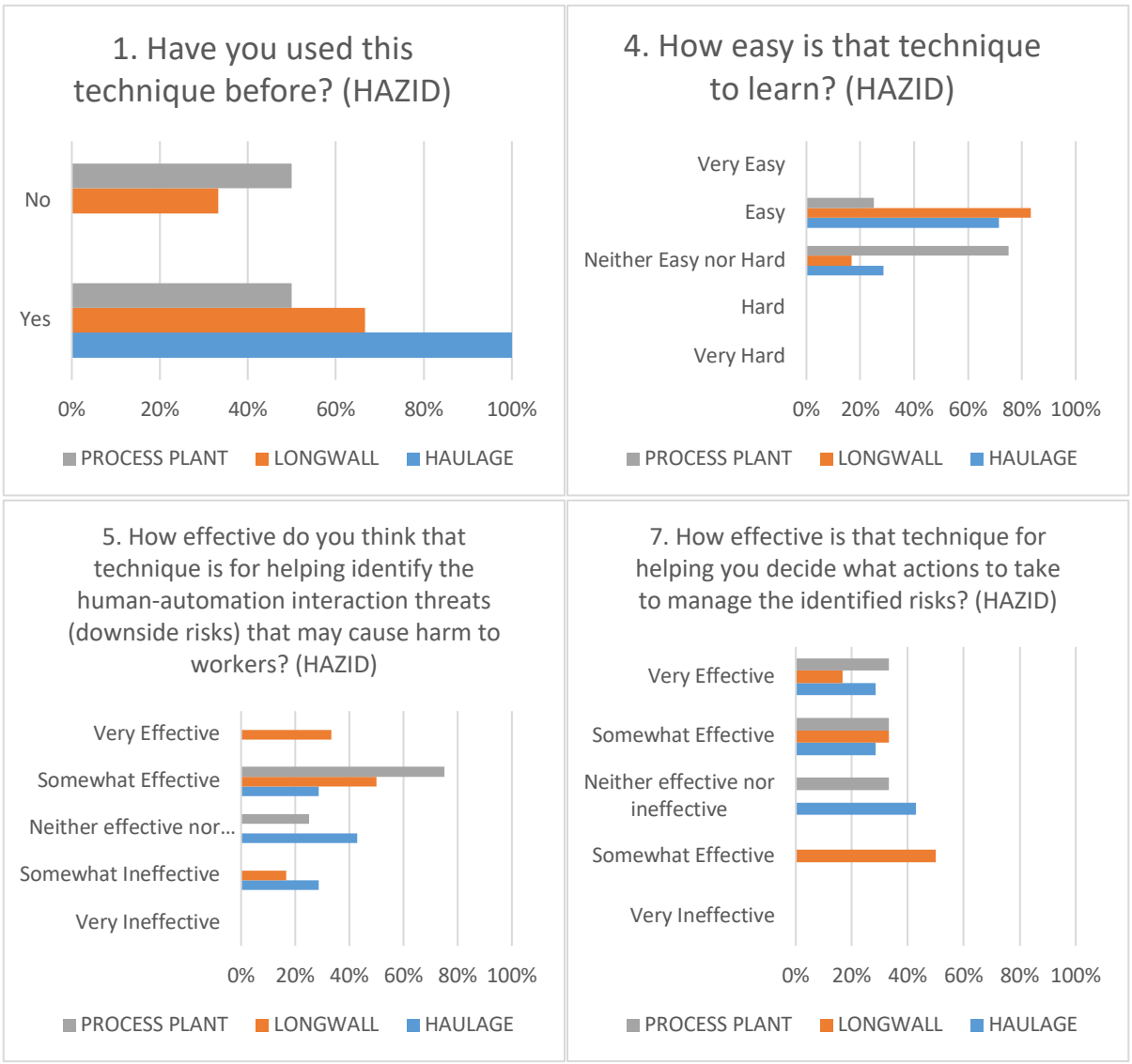


Figure 11: Participant feedback on HAZID process

Participants found the FMECA process as it was applied in the workshops more challenging. Some were familiar with it in other specific situations and when determining corrective actions for equipment failure but they found it challenging to apply to human interactions within a whole system. Comments include it was difficult to identify human-system interaction risks especially in terms of remote vs manned vs autonomous operations. Results from the survey on FMECA are shown in Figure 12.

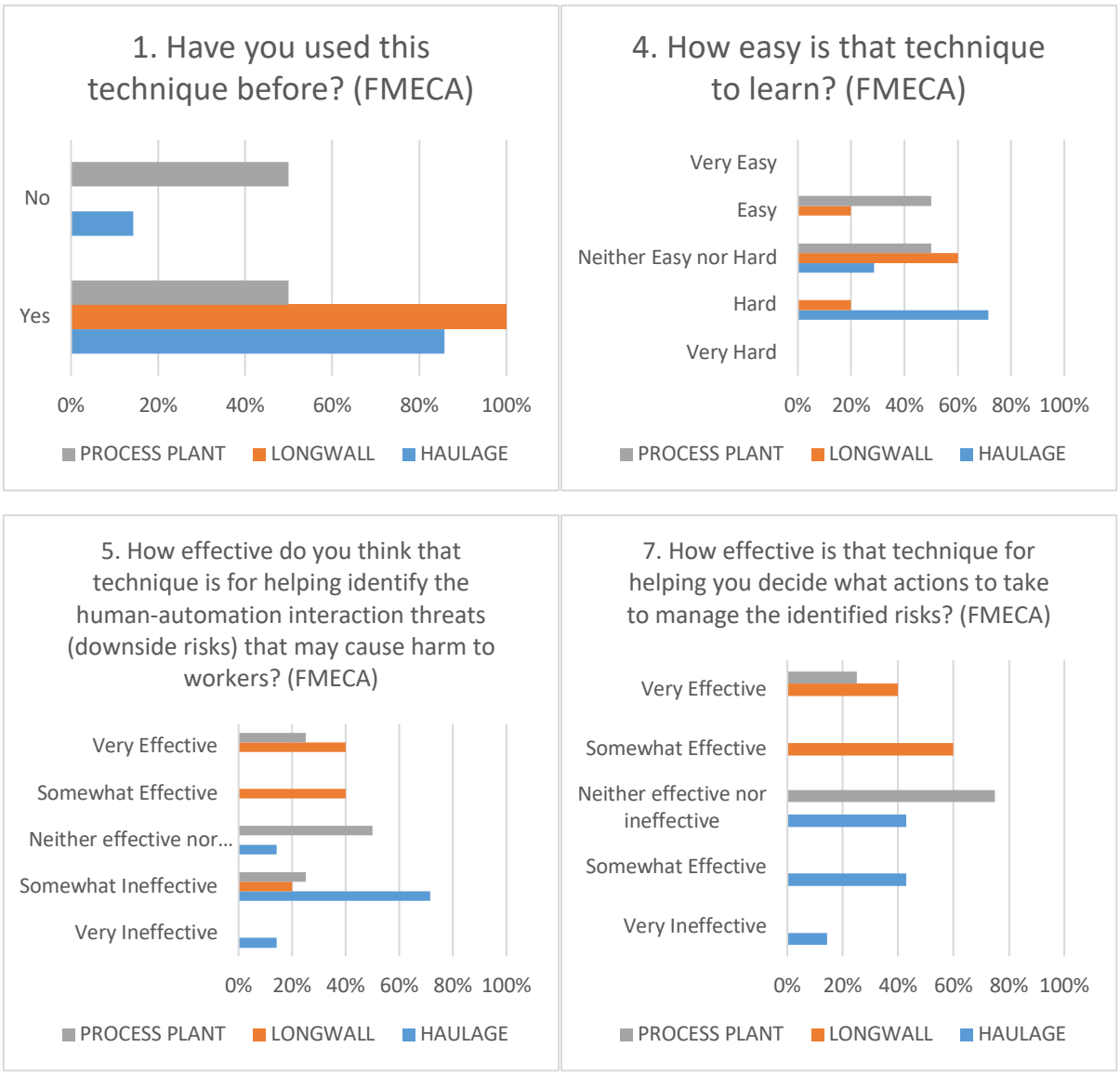


Figure 12: Participant feedback on FMECA

It was most participants' first exposure to SAfER. Comments suggested most found it a good way to identify how to improve system to get human-system interactions safer but they did not see it as a risk assessment process per se. Some suggested it would be good tool to use in conjunction with a more tradition risk assessment tool. Results from the survey on SAfER are shown in Figure 13.

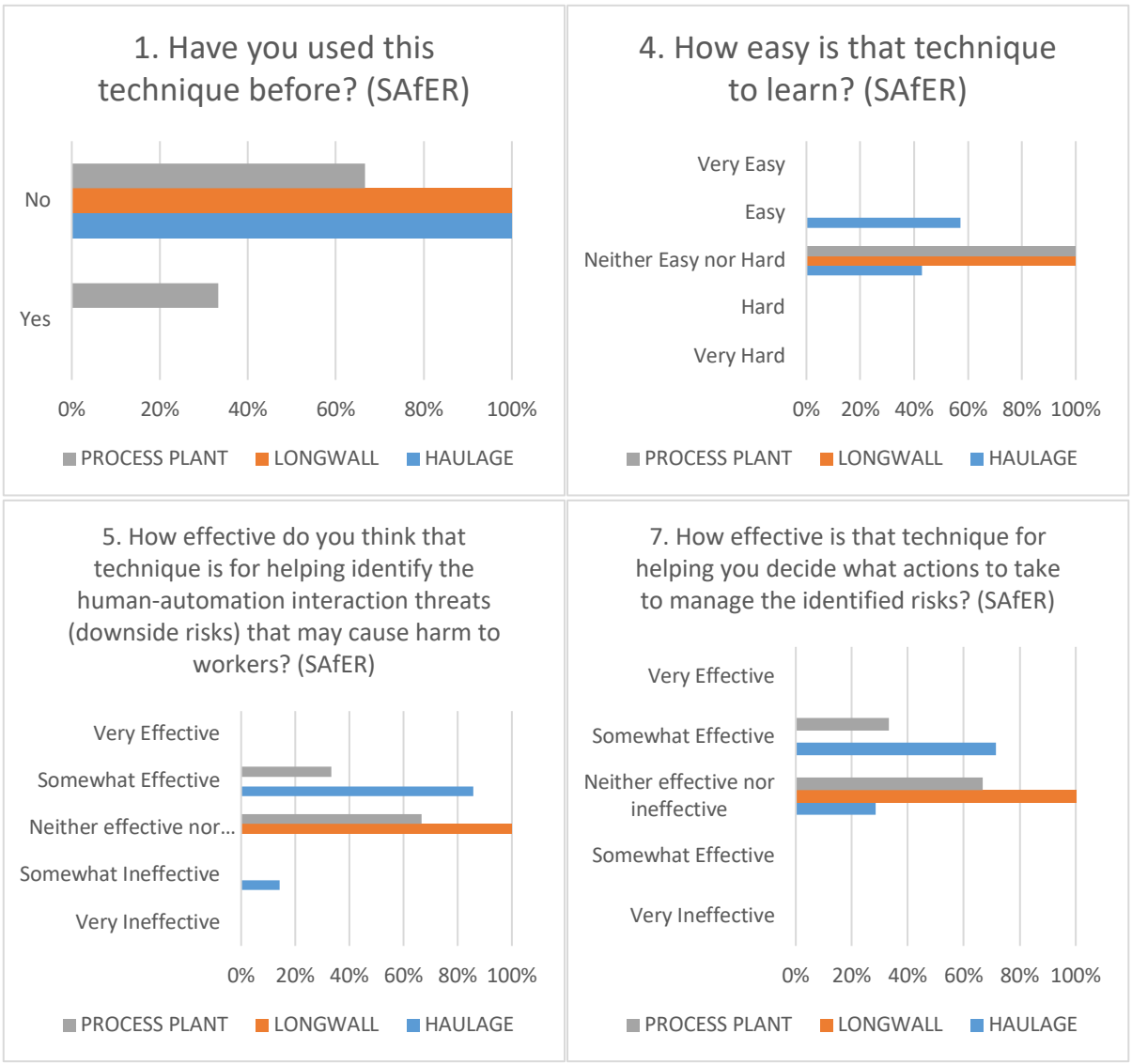


Figure 13: Participants' feedback on SAfER

Most participants had not experienced STPA before. However, comments received suggested that people really liked the process model and some suggested that STPA could be used in conjunction with HAZID to deep dive into the human aspects of high risk scenarios. Results from the survey on SAfER are shown in Figure 14.

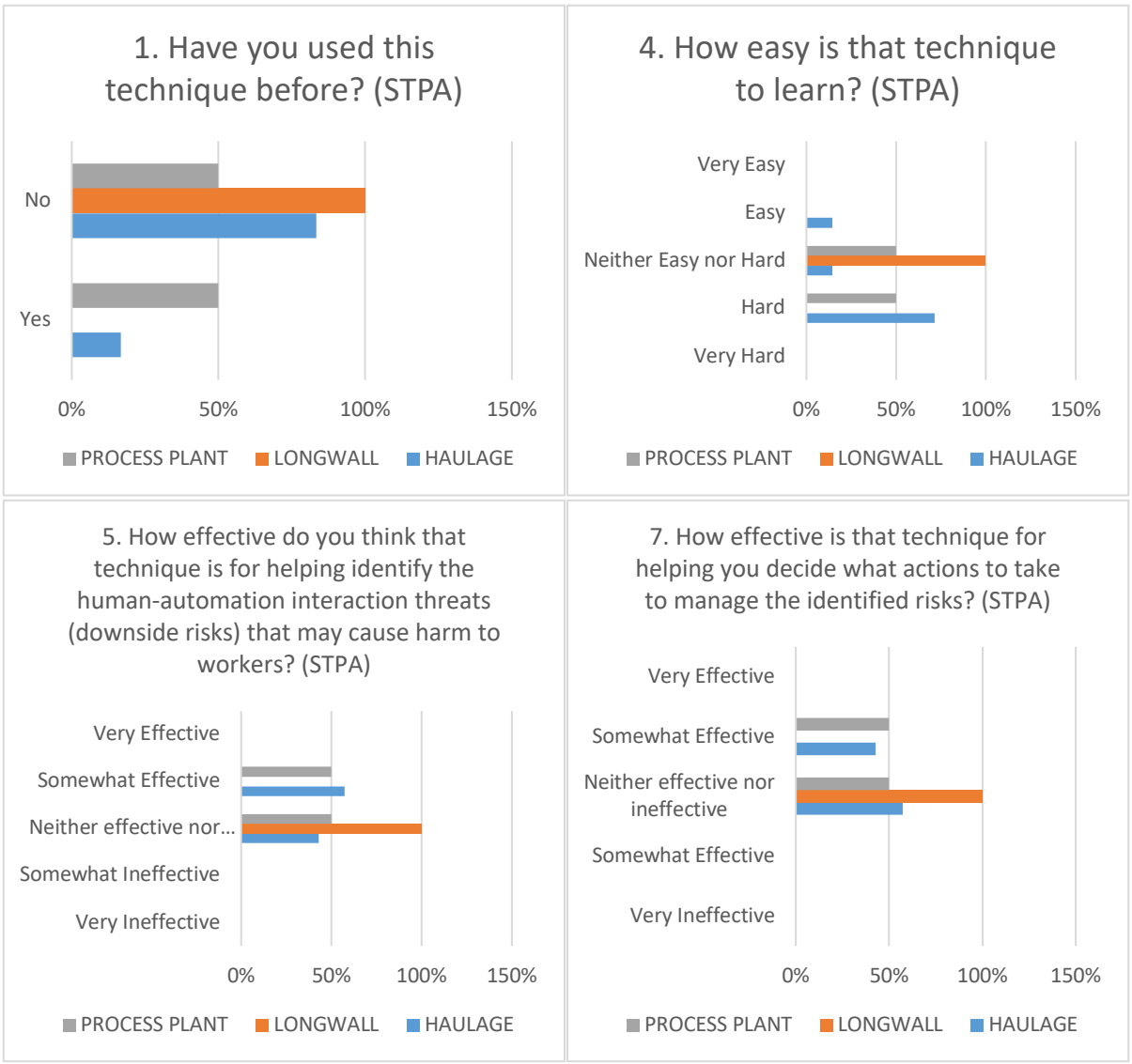


Figure 14: Participants feedback on STPA

Pre and post workshop comparison free- text comments

A number of pre and post workshop comparison free text comments were collected. Key factors were identified factors for helping analysts choose a method for performing hazard identification and risk assessment for systems containing people and autonomous systems interacting. That is, consider the following factors when selecting a method:

- Scope.
    - HAZID suited to broad, less detailed scope for risk assessment.
    - FMECA, SAfER and STPA all were thought to be more applicable to narrower, more detailed scopes. For example:
        - FMECA useful for equipment failures
        - STPA useful for exploring control systems and ineffective control scenarios
        - SAfER useful for understanding and describing how and why people make decisions.
- Ease of use.

    - HAZID was the easiest to use, and the method most participants were familiar with.
    - FMECA/SAfER/STPA were more difficult to use, across the workshops, but yield more detailed results from narrower scopes.
- All methods require facilitation. This is perhaps an obvious point, but it is a key factor often identified for enabling the successful use of a risk assessment method.
- Combination of Methods. Participants mentioned a few times that combining methods, or parts of them, together could be more helpful than using one by itself. For example:
    - Using a risk analysis for decision making around hazards combined with STPA to look at control failures and their contribution to hazard exposure.
    - Exploring both control system dysfunctional interactions and more localised equipment failures.
- Process for the analysis team to go through. Different methods took participants through different kinds of group processes. Choosing what kind of group process organisations may want their risk assessment teams to experience can affect the functionality of the team and the outcomes of their analysis. For example:
    - HAZID – it's less structured than the other method in terms of *how* to go about identifying hazards/controls. It just said you should do that, not how. Some relevant quote include: "It's very subjective"; "Relies on past experience". That is, HAZID is a facilitated discussion around system hazards, with less detailed system decomposition and analysis.
    - FMECA – Equipment failure analysis. A more structured analysis than HAZID. That is, you're focussing the risk assessment team more on one key issue. A different group process than HAZID.
    - STPA – This is more like design thinking, since you have to build a control structure **together**. You're producing an artefact together (control structure). This is a different group process than HAZID or FMECA, and emphasise team building and deeper alignment. Relevant quote about STPA: "*The development of the graphical representation of the control elements is a good way* ***to get alignment with the RA team.****"*
    - SAfER – Being quite a different kind of method from those normally employed in the mining industry for risk assessment, SAfER can **challenge** design teams with getting them to really think about how the operators make decisions, and how to enable better outcomes. Relevant quote: "*Likely to challenge designers more than operators".*

6. Discussion and conclusion

This study had a number of limitations. Due to COVID-19 restrictions in-person workshops were restricted in terms of being able to hold them and the duration that people could spend in one room for a given time. This restriction constrained the ability to fully complete each risk assessment process. The availability of industry personnel was also restricted due to challenges of finding suitably available one-day timeslots to run the workshops. In addition, participation was voluntary so the sampling is biased by those interested in attending. Despite these constraints, all risk assessment processes were able to the trialled with industry practitioners across the three case study scenarios. These risk assessments were able to identify insightful human-system interactions that could be potentially hazardous and therefore warrant further analysis to determine how best to manage them. Feedback from the participants and analysis of workshop information suggest that no single approach is effective any of the case studies nor across the range of automation case studies trialled.

The survey analysis highlighted that SAfER had the highest overall effectiveness score as shown in Figure 15 (also shown in Appendix 1 and Figure A36). Figure 16 also shows

- SAfER had the highest mean, in terms for overall effectiveness of identifying threats, magnitude of impacts and follow up actions.
- STPA was second, then HAZID then FMEA.
- However, again, STPA had the second highest mean but lowest SER.
- All means were above 3, and so in general all participants thought that each method was generally effective.

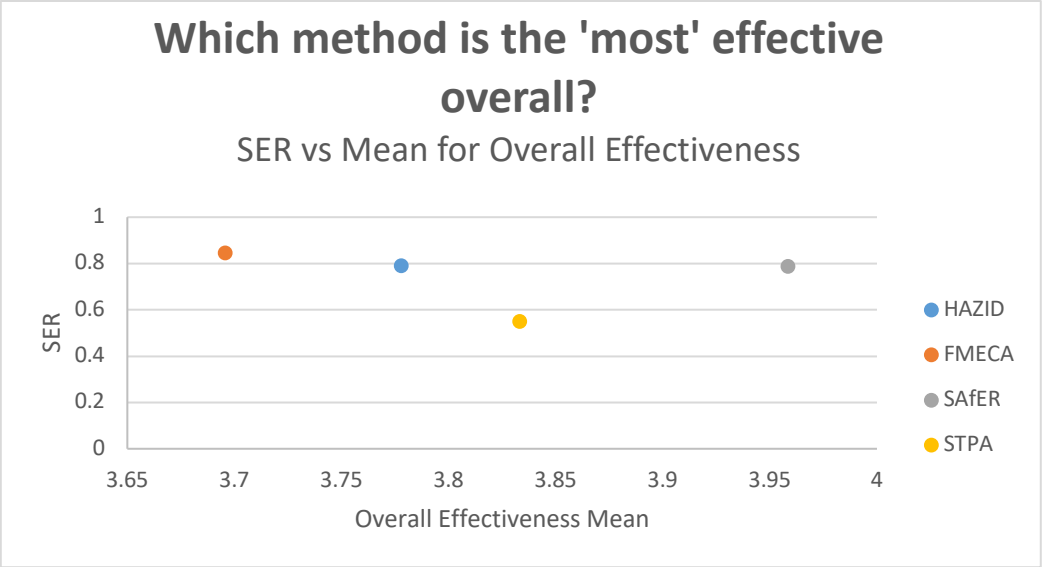


Figure 15: Overall effectiveness rating

Effectiveness is not the whole story, since ease of learning matters as well. For a method to be applied in the workplace, how easy it is to learn is a necessary enabler as well as its actually effectiveness. These two factors (Overall Effectiveness and Ease of Learning) are the two key features to compare these risk assessments methods. Figure A37 shows the comparison between these two variables (which is also shown as Figure 24 in Appendix 1).

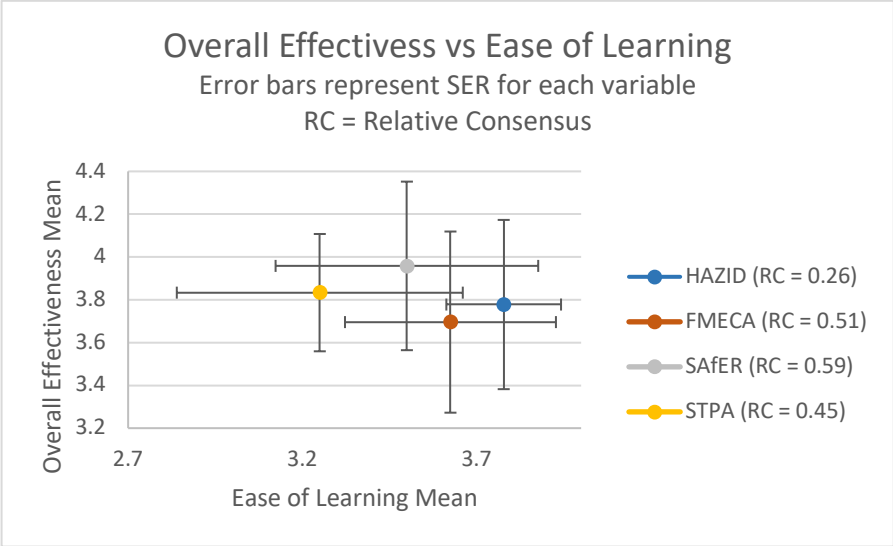


Figure 16 – Comparison of Overall Effectiveness and Ease of Learning for each method

Error bars represent Shannon Entropy Ratio (SER) for "Ease of learning" and "Overall Effectiveness" respectively. The SER represents the consensus for each of these variables – how close or how far from a uniform distribution (no consensus) the results for each method were. The 'area' represented by the combination of both error bars is in indication of the combined consensus about that method over the two key variables: ease of learning and overall effectiveness. Multiplying the SER scores for these two variables gives a 'relative consensus' overall for each method – a representation of this area, as shown in Table 4.

Table 2 – Comparing Ease of Use with Overall Effectiveness, noting Relative Consensus

Method	Mean 'Ease of Learning	Mean "Overall Effectiveness"	Relative 22onsensus (RC) (SER_ease*SER_Effectiveness)
HAZID	3.78	3.78	0.26
FMECA	3.63	3.70	0.51
SafER	3.5	3.96	0.59
STPA	3.25	3.83	0.45

- If we treat effectiveness and ease of learning as equivalently important for a moment, it is plain to see that SafER and HAZID are both the best, as in Figure A37. HAZID for being easiest to learn, and SafER having the highest overall effectiveness. However, SafER had the highest RC (area of the error-bar-square around its mean) and HAZID the lowest.
- HAZID has the lowest SER for Easy of learning, and STPA has the lowest SER for overall effectiveness.
- The fact that the 'area' boxes in Figure A37 overlap is not meaningful in this context, since the error bars don't represent the range of the data, but the SER.

Combining the results of the question analysis with that extract from the free-text comments (shown in Table 5 of Appendix 1), the following are the key conclusions from this analysis:

- Using multiple methods in systems with automation may well be advantageous. For example, note the comments regarding Figure A34. HAZID is easy to use, and perceived as most useful for identifying threats. SAfER was perceived as the most effective for identifying

magnitude of impacts and suggesting follow-up actions. SAfER also had the highest overall effectiveness. However, since the SER for STPA was consistently lower than the other methods, it may well be that SAfER's dominance these areas of effectiveness may well not stand up to further experiments, and as more data is gained STPA may indeed be the preferred method. Additionally, from the comments in Table 3, HAZID is useful for broader scopes and lower required detail, whereas FMECA, STPA and SAfER are naturally narrower in scope but can support a more detailed focus analysis in a particular area: equipment failure, control system design holes and human decision strategies. Different methods are useful for different purposes, and for systems with automation and the diversity of issues, functions and failures they can experience, using a combination of different methods could be the best way forward. It may turn out that only parts of each method may need to be combined with parts of another, rather that perform two or more full analyses. Exploring this more fully should be a key focus of future work.

- The SER score is useful for identifying the most effective method, given a particular survey question. But it is only a clue. Low SER is a clue, not hard evidence, that a method is well understood and has clear consensus for a particular purpose. For example, quite a number of times, STPA had the second highest mean, but lowest SER. Further work should be done on a larger cohort of participants to compare the effectiveness of these different methods, and to find out the significance of the spread of the data on identifying the best method for a given context.

Therefore it is suggested that further work be done to leverage off the feedback provided and investigate a hybrid or combination of approaches might be best the analysis of human-system interactions in mines. Such an approach might consist of:

1. Setting the scope and this should include a human-system interaction diagram (as was produced in STPA).
2. HAZID (for existing systems) or STPA based FMECA (for new systems)
3. Combining the technique from 2. with refined version of SAfER to identify risks and options for reducing those risks.

The STPA based FMECA could comprise the following:

1. Identify the control action from the human-system interaction diagram. Determine relevant failures (including those suggested by STPA).
2. Identify possible causes of the failures
3. Identify possible effects of the failures
4. Assess the effects using the impacts ratings from the risk matrix
5. Assess the likelihood and determine risk rank
6. Recommendations for improving design and/or adding layers of protection (controls) to address those interactions with unacceptable levels of inherent risk.

The refined version of the SAfER process should involve referencing the human-system interaction diagram, performing the situation assessment analysis with the addition of a risk ranking if indicator was absent/overlooked and/or incorrect/misleading. The identification of causes and consequences of strategies along with a risk ranking of them should also be added to the SAfER table.

Appendix A: Survey questions

1. Pre-Workshop Survey Results

2.1 Question 1: Have you used this technique before?

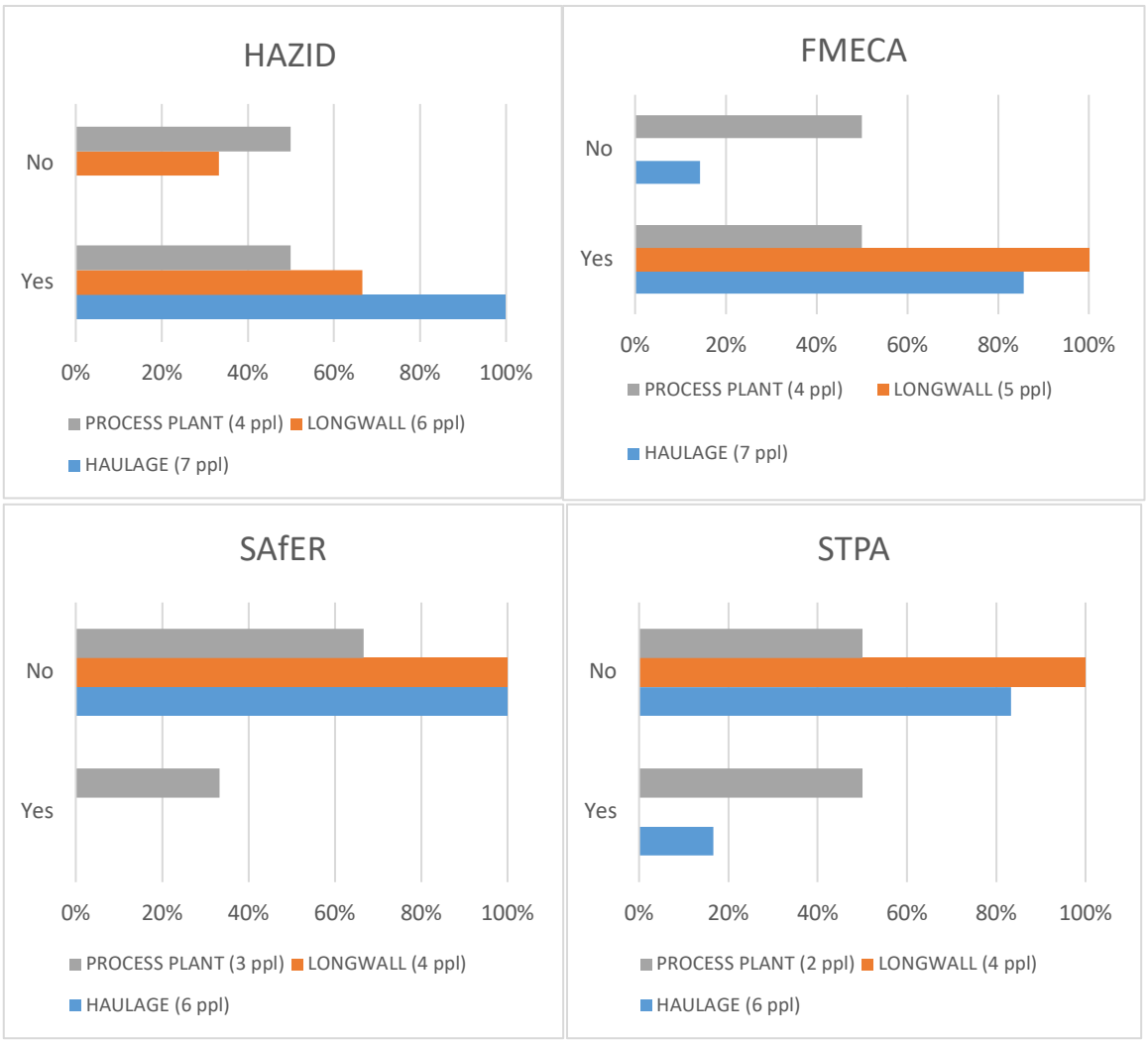


Figure A1 - 1. Have you used this technique before? (Pre-workshop survey)

- The tendency is that HAZID and FMECA were used before, whereas STPA and SAfER were not used before.

2.2 Question 2: Have you been formally trained in this technique?

Figure A15 - 2. Have you been formally trained in this technique? (Pre-Workshop Survey)

- Across all three workshops, half the cohorts were trained in HAZID and FMECA, and half weren't.
- No workshops participants were trained in SAfER or STPA.

2.3 Question 3: How regularly would you (approximately) use this technique?

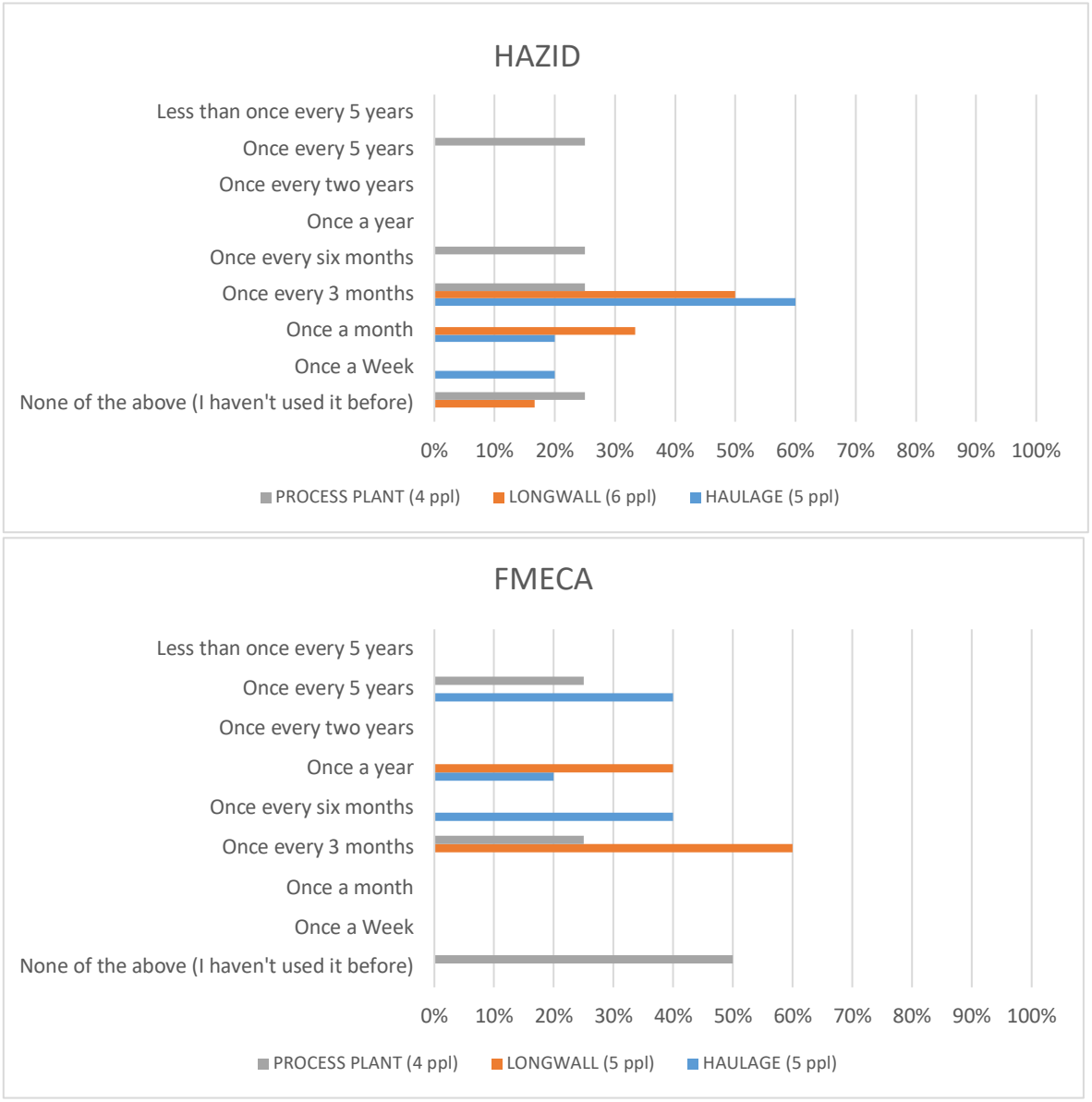


Figure A16 – 3a. How regularly would you (approximately) use this technique? – HAZID and FMECA (Pre-workshop survey)

Figure A17 – 3b. How regularly would you (approximately) use this technique? – SAfER and STPA (Pre-workshop survey)

- In alignment with responses from Figure and Figure A15, SAfER and STPA were not really used by the workshop participants, as shown in Figure A17.
- HAZID and FMECA, which were used before, showed a wide distribution of how often they were used. HAZID was previously used more often than FMECA (higher apparent mean, although this was not calculated – the values area essentially cardinal, not ordinal, even though they are frequencies).

2.4 Question 4: How easy is that technique to learn (e.g. is specialists training or facilitation required to do a good risk assessment)?

Figure A18 - 4. How easy is that technique to learn? (Pre-workshop survey)

- In general, before the workshops, participants thought that HAZID and FMECA were easier to learn than SAfER or STPA (look at mean values).
- Not many people had used SAfER before. That is likely why they put 'Neither Easy nor Hard'. The comments on SAfER from Table 5 indicate that the answers for SAfER for questions 4, 5, 6 and 7 are not particularly meaningful, in the pre-workshop survey, since some participants haven't used it before.
- Only 1 participant from the process plant workshop had used STPA before, and presumably, according to Figure A18, thought it was hard to learn. A few people from the Haulage

workshop also thought it was hard to learn. It is perhaps these participants who also thought FMECA was hard.

- The Haulage workshop thought SAfER might be easier to use than FMECA, even though they hadn't used it before.

2.5 Question 5: How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers?

Figure A19 - 5. How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers? (Pre-workshop Survey)

- For both HAZID and FMECA, there is wide distribution in terms of whether participants thought they'd be effective for identifying threats. Participants perceived HAZID to be, in general, more effective that FMECA.
- Because most participants hadn't used SAfER or STPA before, the distribution of responses are much narrower than for HAZID or FMECA. They were just the central values of "Neither effective nor ineffective". The SAfER and STPA results were very similar – these were perceived as slightly effective for idnetifying these threats.

- It is hard to compare the results between HAZID/FMECA and SAfER/STPA since participants hadn't, in general, used SAfER or STPA to the same extent as HAZID/FMECA. Therefore, the knowledge base/experience were different between these two sets of methods, making conclusions drawn before the workshops, less meaningful.
- Longwall participants thought both HAZID and FMECA were quite effective, whereas Haulage participants perceived HAZID as neutral and FMECA to be on the ineffective side. The process plant participants thought both tended to be effective.
- HAZID had the highest consensus for process plant participants.
- FMECA had highest consensus for Haulage
- STPA: all 3 workshops' participats were either neutral or positive. SAfER was similar, in the means, although one person from the Haulage workshop thought it might be somewhat ineffective.

2.6 Question 6: How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks?

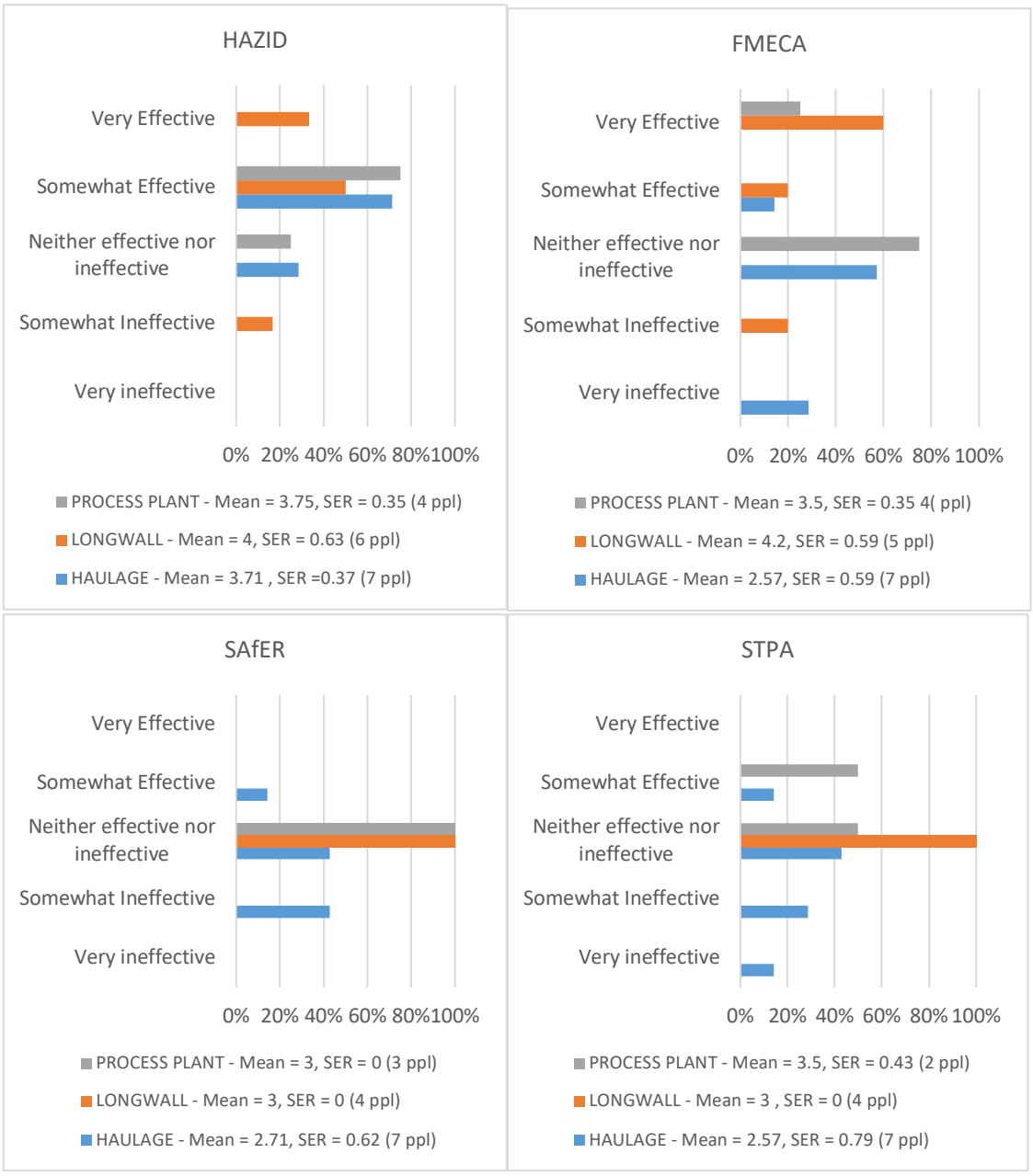


Figure A20 - 6. How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks? (pre-workshop survey)

- HAZID had a narrower distribution overall (in terms of maximum and minimum values) than FMECA. More overall concensus about effectiveness of HAZID for identifying impacts.
- STPA had a wider distribution than SAfER.
- With the exception of HAZID, Haulage participants tended to rate all method on the neutral or ineffective side, since the means were all less than 3. Haulage participants had greater consensus about HAZID than the other methods (low SER).
- Process plant and longwall participants rated all methods as more effective than Haulage participants.

2.7 Question 7: How effective is that technique for helping you decide what actions to take to manage the identified risks?

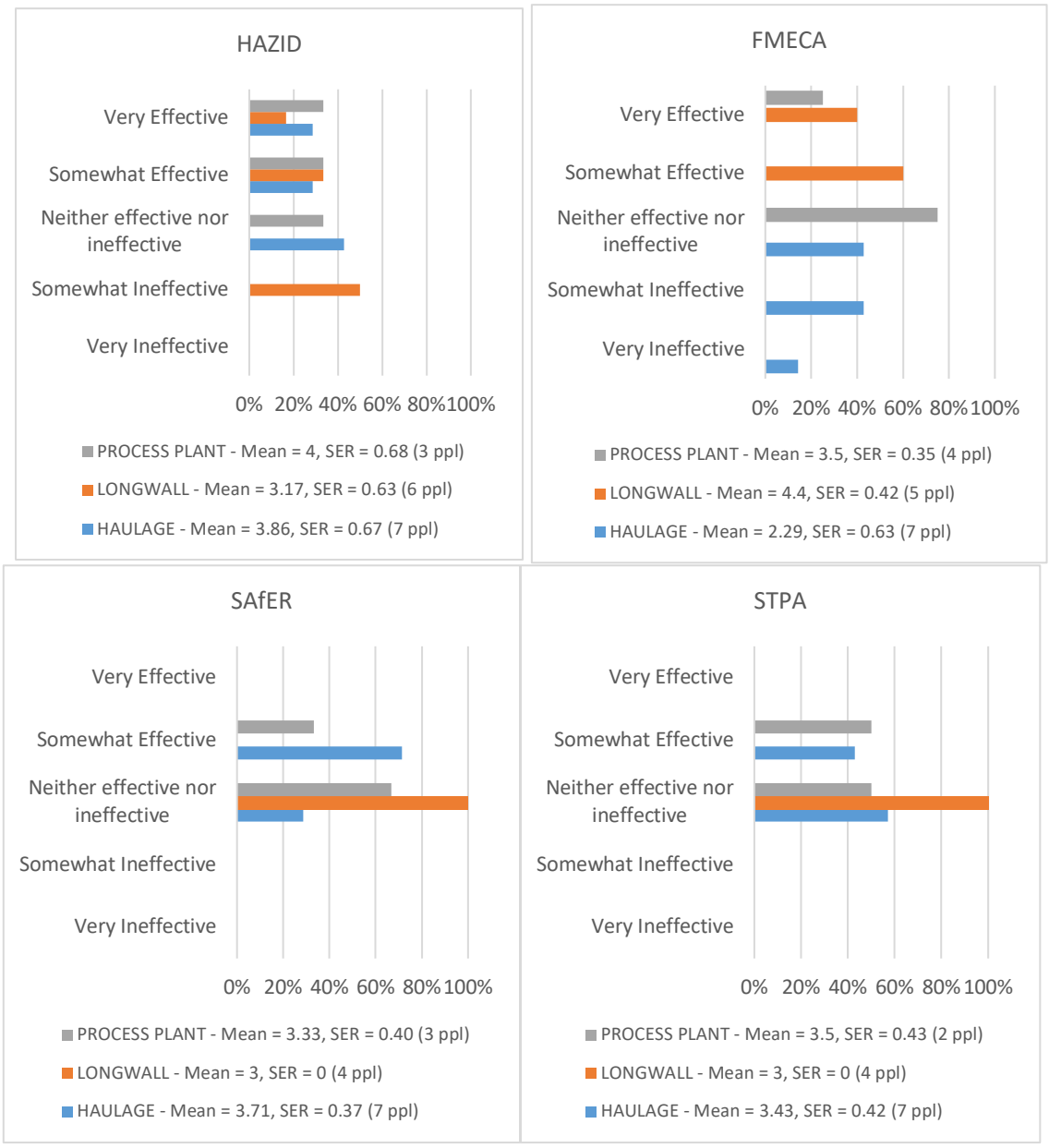


Figure A21 – 7. How effective is that technique for helping you decide what actions to take to manage the identified risks? (pre-workshop survey)

- SAfER and STPA results are very similar – slightly on the effective side. But it appears all participants were more unsure about the effectiveness of these methods for identifying actions. Especially since many participants have not used SAfER and STPA before. There were lots of neutral results - e.g. longwall.
- HAZID and FMECA had wider distributions than SAfER and STPA.
- Haulage participants thought FMECA much less effective than HAZID, as seen in the means in Figure A21. The SER for Haulage HAZID and FMECA are very similar (0.67 and 0.63 respectively). The similar SER indicates that the whole distribution has shifted down from the HAZID to FMECA. This is also seen visually in Figure A21. A different mean, but the same SER, between two distributions can indicate a large shift in the overall consensus as to the

value of a variable. This is because the means hasn’t just moved because some participants have differnet perceptions, but that most or all of them do.

3 Pre-and-Post Comparison (Longwall and Process Plant)

This is for the Longwall and Process Plant only. The post-survey results for Haulage were not collected. This section of analysis is to explore whether participants changed their perception about the methods as a results of attending the relevant workshop.

e. 3.1 Question 1: How easy is that technique to learn?

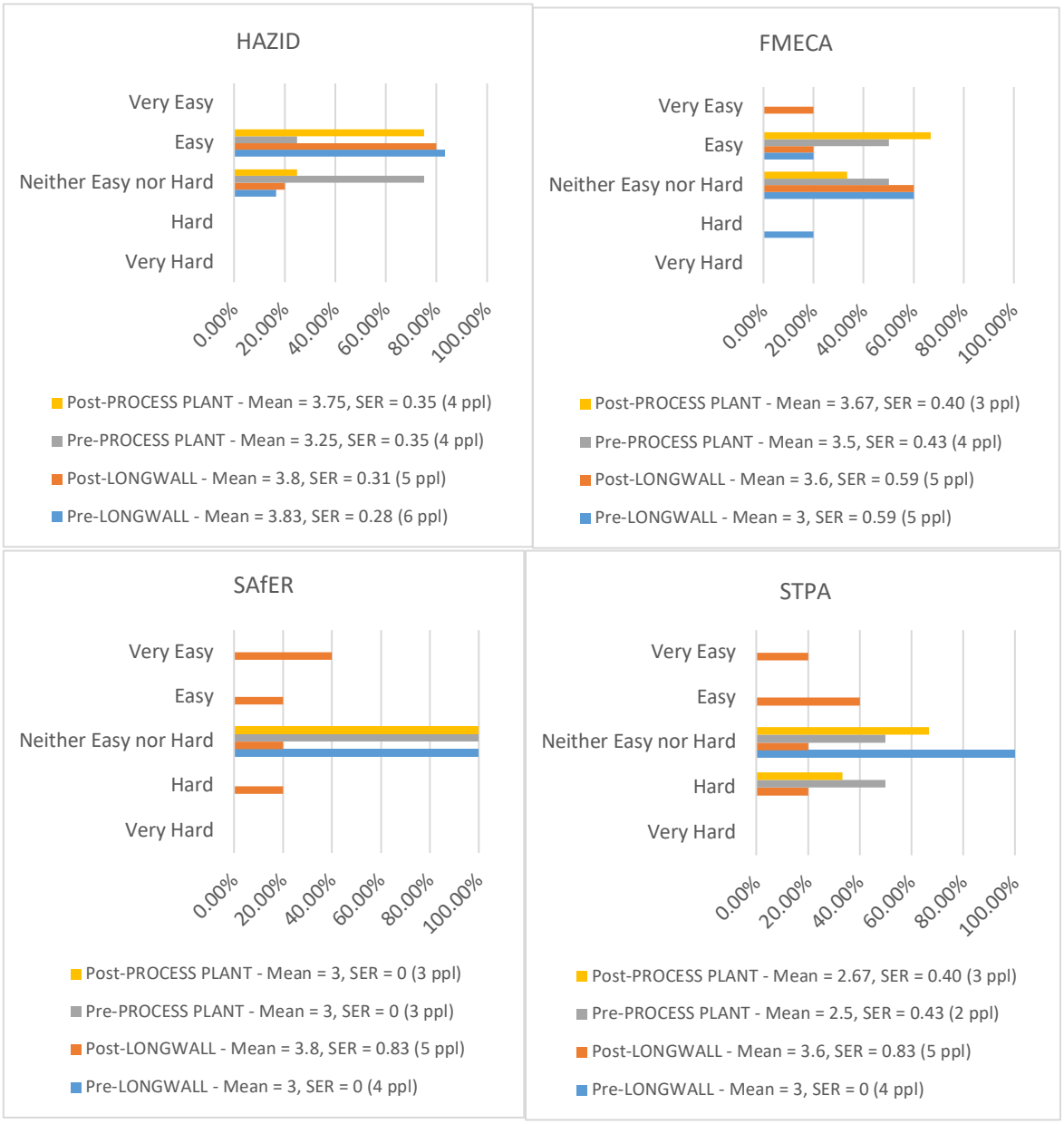


Figure A22 - 1. How easy is that technique to learn? (post-workshop survey)

- For HAZID, pre-longwall and post-longwall were similar in how hard participants thought it was to use (similar means and SER). Pre-process plant and post-process plant were the opposite – after the workshop, participants thought it was easier than their pre-workshop opinion. See shift in mean and same SER, indicating a clear shift in consensus perception of the group.
- For FMECA, similar to HAZID, post-workshop participants thought it was easier that originally perceived. This was shown clearly with the Longwall results: shift in mean with same SER.

However, with the Process Plant, only 3 instead of 4 people responded after the workshop, so it is not clear if perceptions did change, or one participant chose not to answer.

- For SAfER, post-workshop Longwall participants thought it was on the easy side, on average. Process Plant participants were unchanged in their opinion.
- For STPA, post-workshop Longwall participants thought it was easier than the thought before, and post-workshop Process Plant participants were relative unchanged – although one extra person answered the post-workshop survey. There were more people that for the other methods, that thought STPA was harder to use.

3.2 Question 2: How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers?

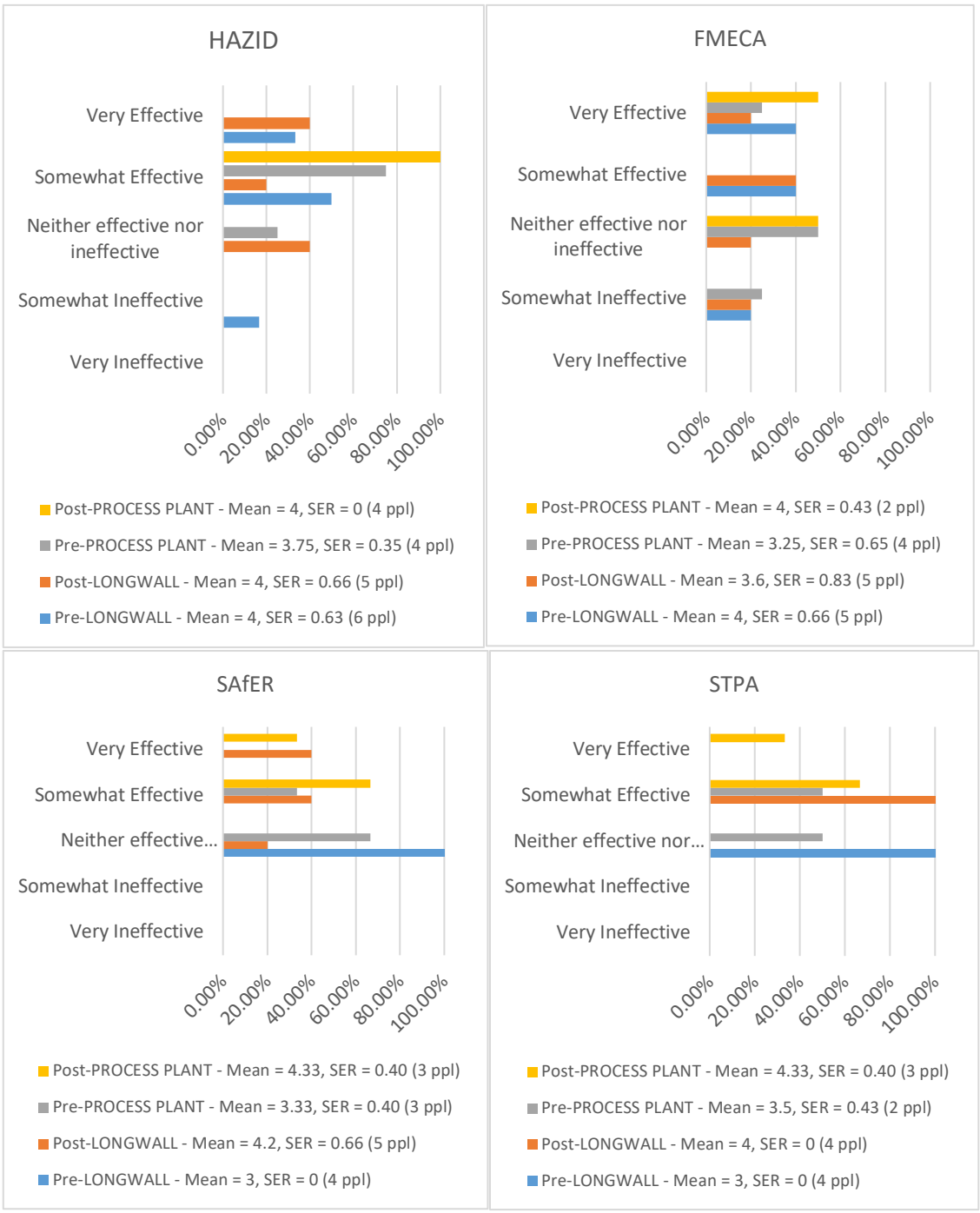


Figure A23 - 2. How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers? (post-workshop survey)

- HAZID: Longwall participants had no change. Process Plant increased in mean and consensus (higher mean and lower SER).
- FMECA, post-workshop, Process Plant participants thought it was more effective that originally thought. However, 2 less people answers the process plant post-workshop survey, so the increase in mean may be a result of that. Longwall participants decreased their

opinion of FMECA post-workshop. But this was coupled with a higher SER – less consensus. It appears, from Figure A23, that one person from the longwall workshop changed their opinion, and all other stayed the same.

- In spite of being more unfamiliar with STPA and SAfER before the workshops, participants thought they were both quite effective at identifying threats. For both Longwall and Process Plant workshops, perceptions increase (as more effective) considerably. For SAfER for the longwall group, the SER increased a lot as well, indicating the some people kept the same opinion, and others changed, thinking SAfER more effective that originally thought. For STPA and the Longwall group, the SER was the same, indicating a clear increase in perception.

3.3 Question 3: How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks?

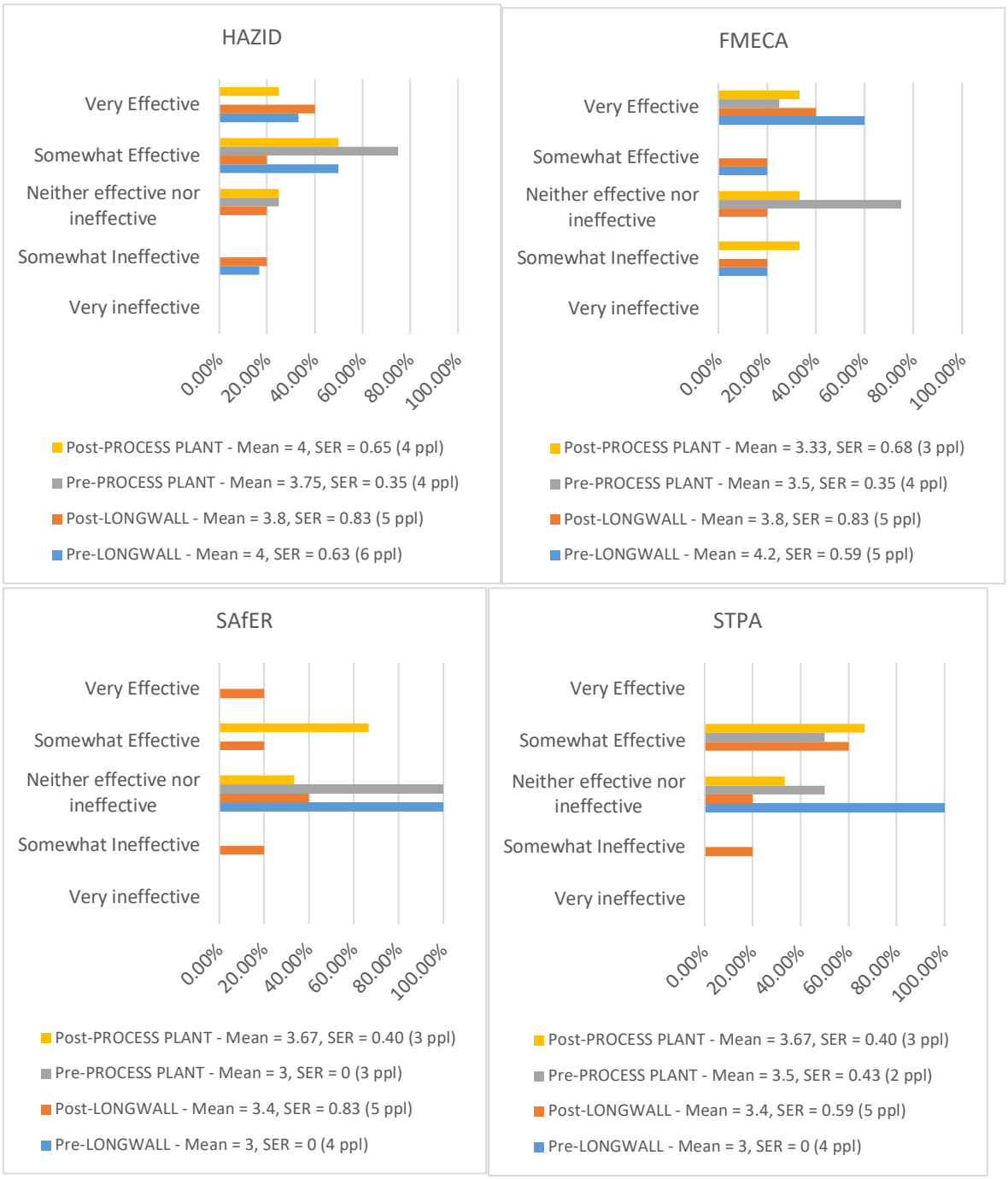


Figure A24 - 3. How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks? (post-workshop survey)

- HAZID: for the longwall group, there was a decrease in mean and increase in SER, meaning a few, but not all, participants changed their opinion. For process plant, the opinions shifted, and participants thought HAZID was more effective post workshop than pre, although only a few parcipants changed opinion (increase in SER).
- FMECA: for longwall, the perception dropped slightly post workshop. The SER increased, so some people changed opinions. For the process plant, the pre perception was neutral, but

post workshop the perceptions split – some remaining neutral, one very favourable and one more negative.

- SAfER perceptions shifted a lot pre and post workshop, for both longwall and process plant. Generally shifting towards the more effective side. Both workshop groups had a higher SER post-workshop. This represents the fact that pre-workshop participants didn't know the method, and thus probably put "Neither effective nor ineffective" as a default position.
- STPA opinions didn't shift pre and post for the process plant. An extra person responded to the latter workshop, changing the distribution slightly. It was perceived as effective. For the longwall workshop, post-workshop participants generally thought that the method was on the effective side.

3.4 Question 4: How effective is that technique for helping you decide what actions to take to manage the identified risks?

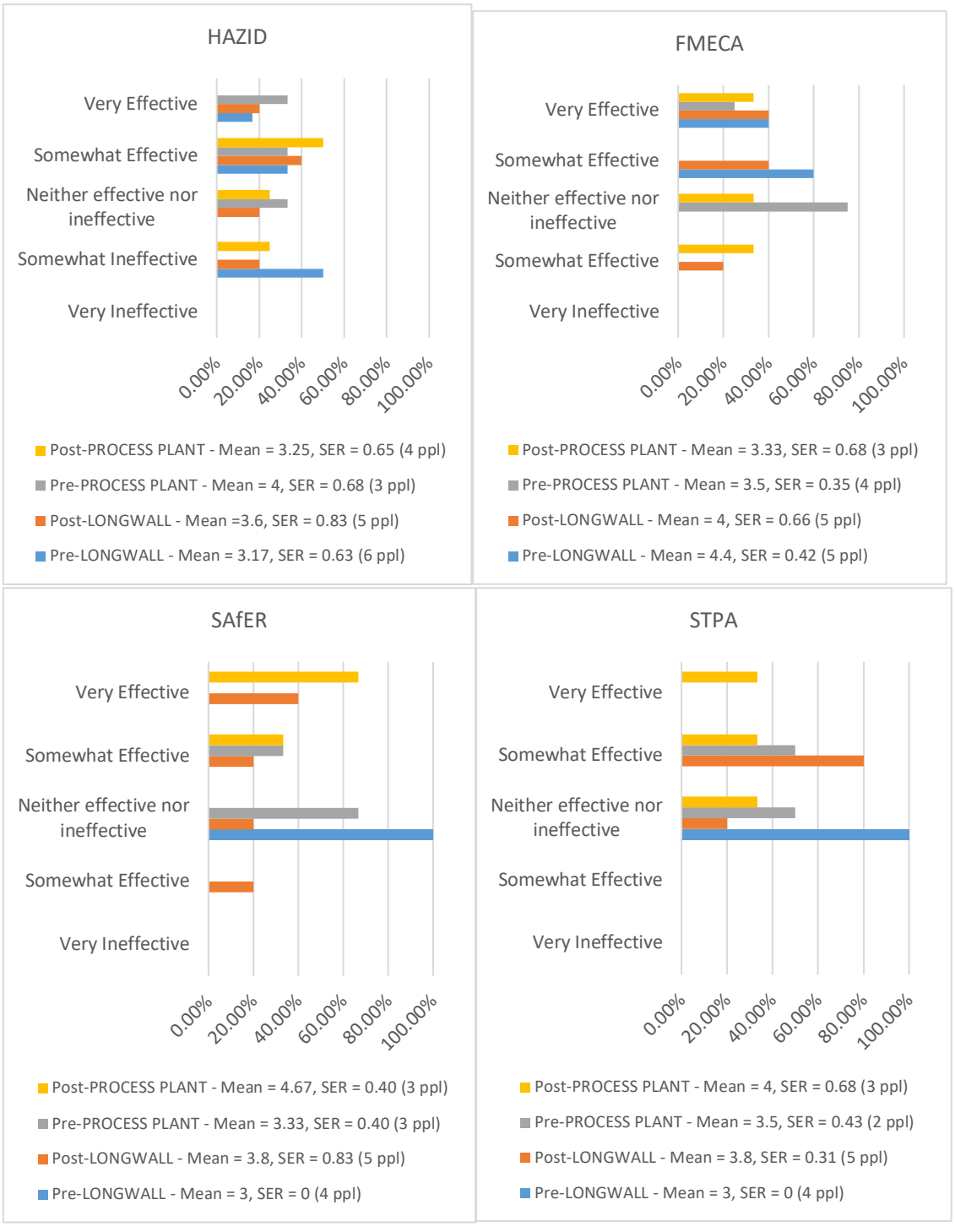


Figure A25 - 4. How effective is that technique for helping you decide what actions to take to manage the identified risks? (post-workshop survey)

- HAZID: Longwall increase in mean post-workshop. Even though one less participant answered post-workshop, at least one participant who thought it was somewhat ineffective pre-workshop, shifted up to neutral. The process plant participants decreased their opinion, although this may be explained by the one less participant answering post-workshop.

- FMECA: post-workshop, one longwall participant decreased their opinion, explaining the drop in mean and increase in SER. Process plant post-workshop had one less answer, but in spite of this it is possible to see that one participant did decrease their opinion.
- SAfER: Big increase for both longwall and process plant post-workshop. Both groups thought that SAfER was much more effective than originally thought. The much bigger SER for longwall post-workshop occurred because before the workshop people didn't know about the method, but afterwards they did and their actual perceptions emerged.
- STPA: Big increase in perceived effectiveness post-workshop for longwall. Most of the neutral perceptions moved to 'somewhat effective'. Process plant perceptions also increased, and addition of an extra person's answers strengthens the conclusion of the increased mean.

Method comparisons for Post-Workshop Surveys (Longwall and Process Plant only)

f. 4.1 Question 1: How easy was the method to learn?

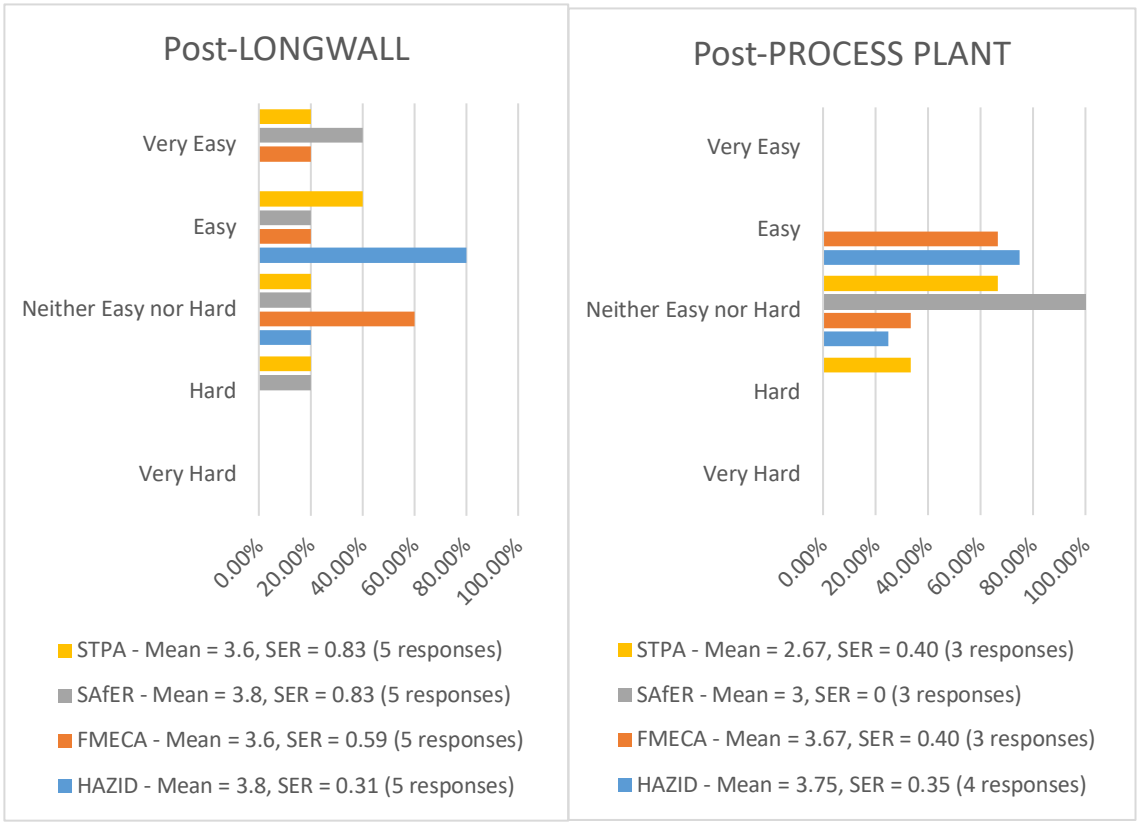


Figure A26 - 1. How easy is that technique to learn? (post-workshop survey) (comparing all methods for longwall and process plant separately)

- Post-workshop Longwall, most participants thought that HAZID and SAfER were easier to learn than FMECA and STPA (see means). Only SAfER and STPA had 'hard' ratings post-workshop longwall. However, the SER for HAZID was much lower, meaning there was more consensus than SAfER.
- Post-workshop Process plant, participants thought that HAZID and FMEA were easier to use – these were the only two methods that got 'easy' ratings. STPA got a 'hard' rating, and SAfER was 'neither easy nor hard. STPA was perceived as the hardest to use. The SER of all scores was reasonably low.
- For the post-workshop for longwalls, STPA and SAfER were seen as hardest to use, and also very easy to use – this is individual person specific. The SER was very high for both, indicating there was low consensus it the group about these methods.
- FMECA was also on the easy side, but had a wider distribution than HAZID and less wide than SAfER and STPA. Someone in the longwall workshop thought FMECA was very easy to use for that application.

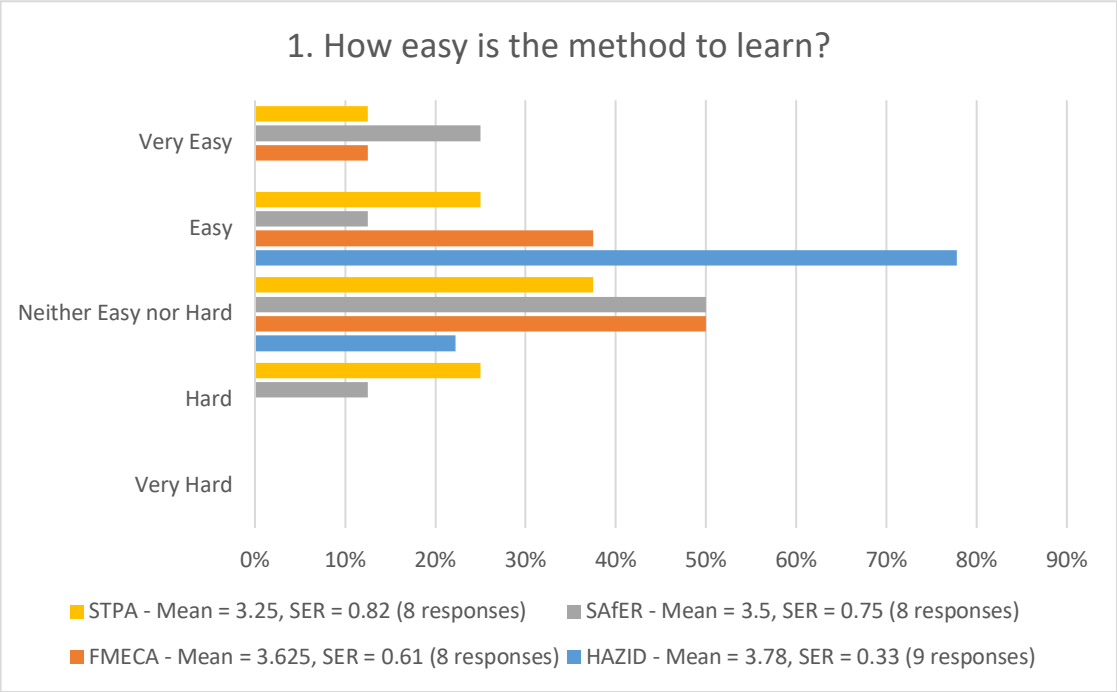


Figure A27 - 1. How easy is that technique to learn? (post-workshop survey) (comparing all methods for longwall and process plant combined)

- Combining the responses from both workshops, HAZID was seen as easy most consistently (highest mean). All other methods had a much wider distribution than HAZID, showing lower consensus with those methods.
- The two traditional methods (HAZID and FMECA) were seen as easier to learn than the two newer, system-theory based methods (STPA and SAfER).
- FMECA was the 2nd easiest to learn, followed by SAfER then STPA. The order is very clear, although with each method in mean order, the SER increases, meaning that consensus decreases.

4.2 Question 2: How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers?

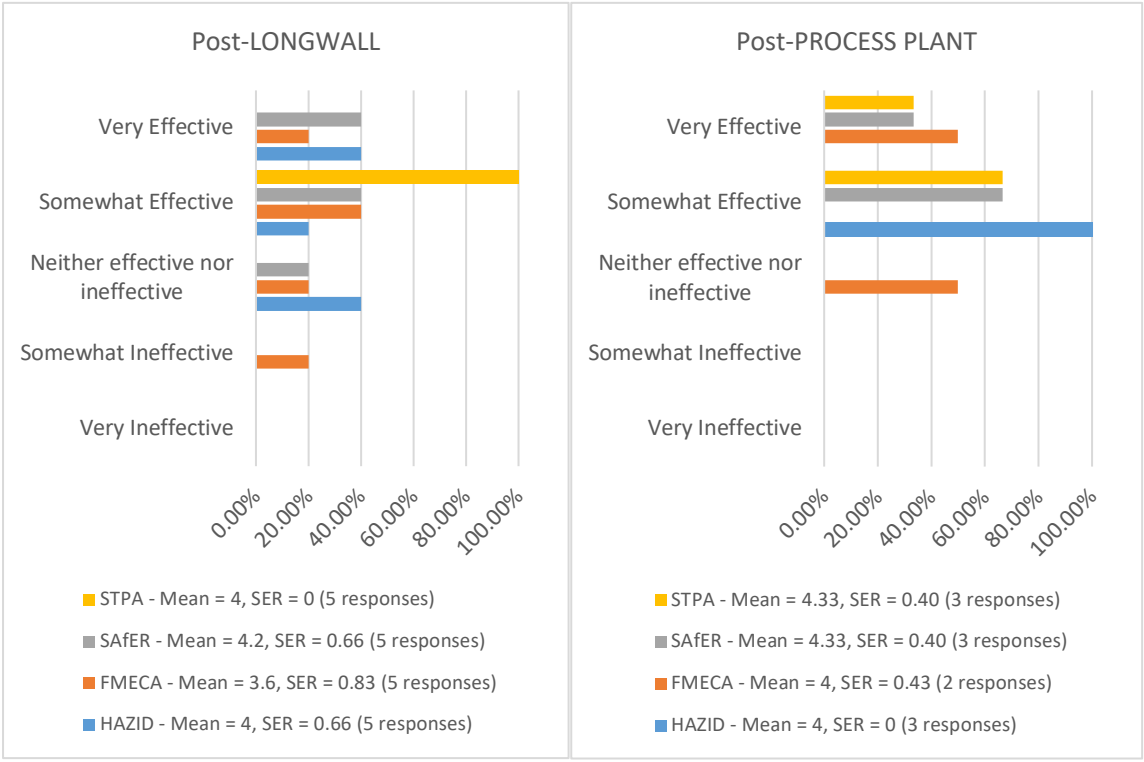


Figure A28 - 2. How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers? (post-workshop survey) (comparing all methods for longwall and process plant separately)

- Post-workshop longwall, SAfER has the highest mean. STPA was next highest, but its SER was much lower than SAfER's. This indicates that participants were much more sure, that STPA was effective for the application, but they were less sure about SAfER. HAZID and STPA were equally second highest, but the SER for STPA was much lower than HAZID, putting STPA clearly as the second-highest.
- For the post-workshop Process Plant, STPA and SAfER were percecived as the most effective at identifying threats. There were more concensus about STPA and SAfER than FMECA, but HAZID had the lowest SER.
- In both cases FMECA was perceived as the least effective, either in terms of lowest mean (Longwall), or equal-lowest mean but a higher SER (process plant). Since there were only 2 responses for FMECA, and only 3 for the other methods for the process plant, the significance of SER scores should be treated with caution.

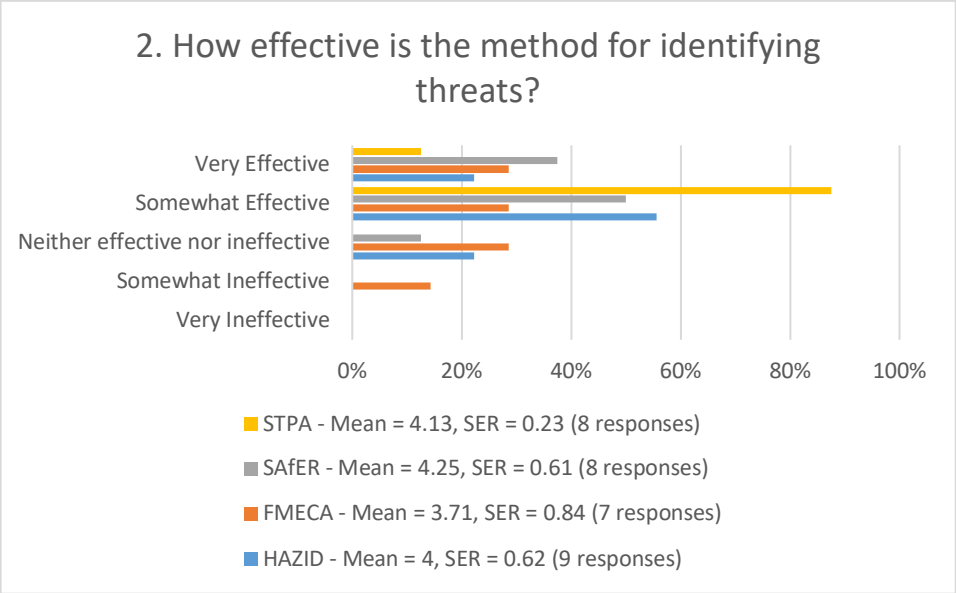


Figure A29 – 2. How effective do you think that technique is for helping identify the human-automation interaction threats (downside risks) that may cause harm to workers? (post-workshop survey) (comparing all methods for longwall and process plant combined)

- From Figure A29, when combining all the workshops results together, SAfER has the highest mean. However, STPA, with the next highest mean, had a much lower SER score. Therefore, it could be argued that either method could have been perceived as the most effective.
- HAZID was perceived as having an effectiveness next after STPA and SAfER, with FMECA lowest. Again, the SER for FMECA was very high, showing lower consensus for that method.

4.3 Question 3: How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks?

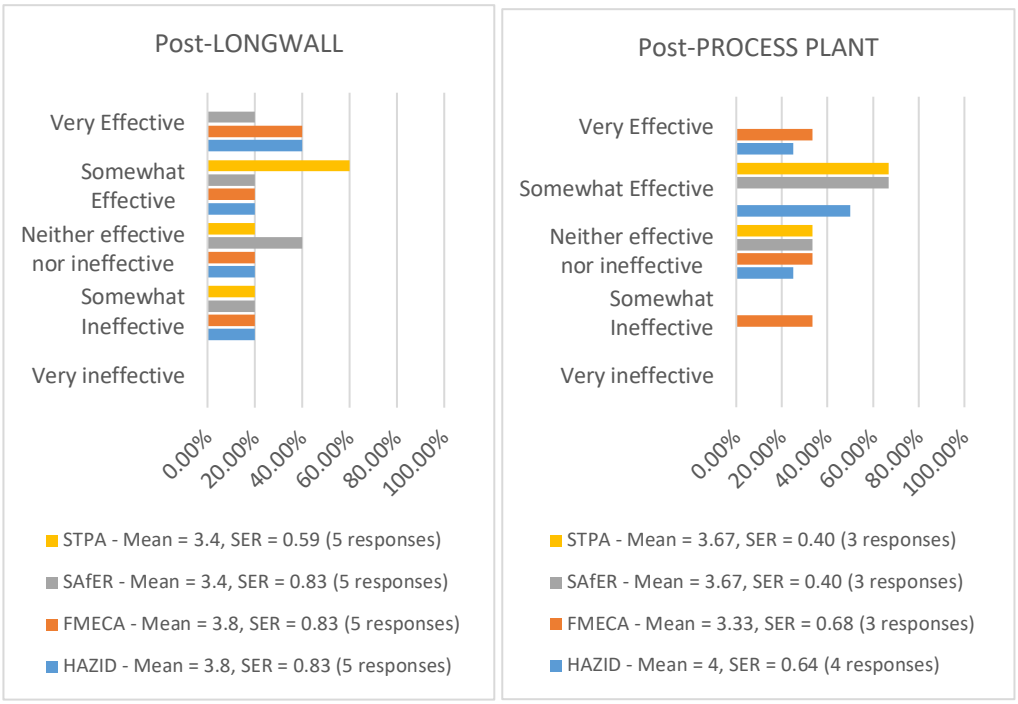


Figure A30 – 3. How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks? (post-workshop survey) (all methods together with longwall and process plant separately)

- For Post-workshop longwall, HAZID and FMECA had the highest means, and almost equal SER's. They had very high SER's. STPA had the lowest SER, and thus the most consensus, although its mean was lower than HAZID/FMECA.
- HAZID had the highest mean for the post-workshop process plant, followed by STPA and SAfER equal and then FMECA last.

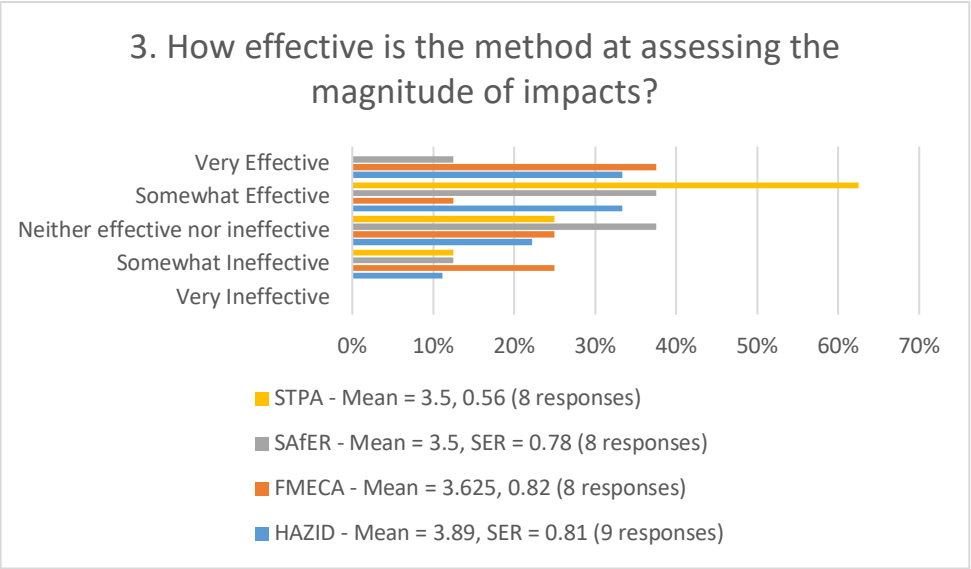


Figure A31 - 3. How effective is that technique for helping you assess the magnitude of potential impacts of the human-automation system interaction risks? (post-workshop survey) (all methods combined with longwall and process plant combined)

- HAZID has the highest mean, followed by FMECA, and then STPA and SAfER are equal lowest. HAZID's SER is quite high, so the consensus about it to identify magnitude of impacts was low.
- STPA has the highest SER and thus the most consensus.
- FMECA and SAfER had high SER's, and thus consensus was split about whether they were effective or not.

4.4 Question 4: How effective is that technique for helping you decide what actions to take to manage the identified risks?

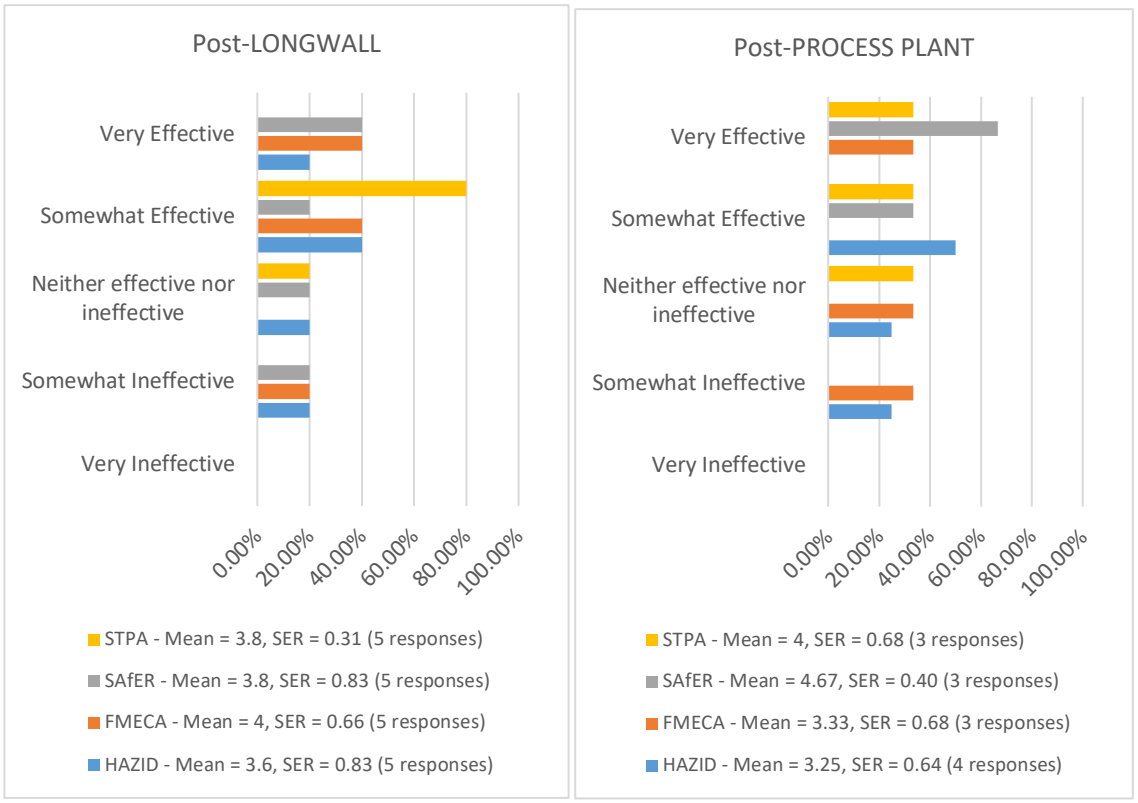


Figure A32 - 4. How effective is that technique for helping you decide what actions to take to manage the identified risks? (post - workshop survey) (methods combined for longwall and process plant separately)

- Longwall – FMECA has the highest mean, followed by STPA and SAfER equally, then HAZID as the lowest. However, FMECA has a higher SER than STPA. There is more consensus about the effectiveness of STPA to choose actions than FMECA.
- Process plant – SAfER had the highest mean and lowest SER. Consensus was high that SAfER helped identify actions for this case study, although there were only 3 responses.

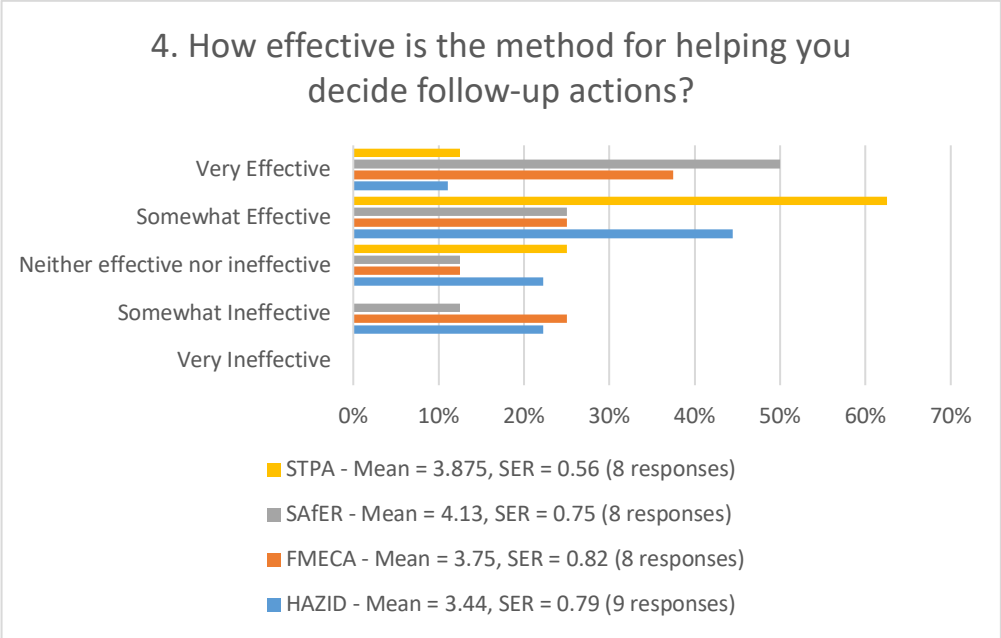


Figure A33 – 4. How effective is that technique for helping you decide what actions to take to manage the identified risks? (post – workshop survey) (methods combined for longwall and process plant combined)

- SAfER had the highest mean overall. STPA was second, but had a lower SER than SAfER. Therefore, it is possible either SAfER or STPA could be considered the most effective in general.

Table 3 displays all of the means and SER's for each method for each question asked. These are the combined means from both the post-workshop longwall and process plant surveys. Figure A34 shows plots of Mean vs SER for each method for each question. This was to explore patterns between the methods, giving a visual aid for identifying which might be the best method for use with systems having automation.

Table 3 – Mean and SER for each method for each question (post-workshop, combination of longwall and process plant) (Dark green is Highest score on each line, red is lowest)

	HAZID		FMECA		SAfER		STPA	
	Mean	SER	Mean	SER	Mean	SER	Mean	SER
1. How easy is the method to learn?	3.78	0.33	3.63	0.61	3.5	0.75	3.25	0.82
2. How effective is the method for identifying threats?	4	0.62	3.71	0.84	4.25	0.60	4.13	0.23
3. How effective is the method at assessing the magnitude of impacts?	3.89	0.81	3.63	0.82	3.5	0.78	3.5	0.56
4. How effective is the method for helping you decide follow-up actions?	3.44	0.79	3.75	0.82	4.13	0.75	3.88	0.56

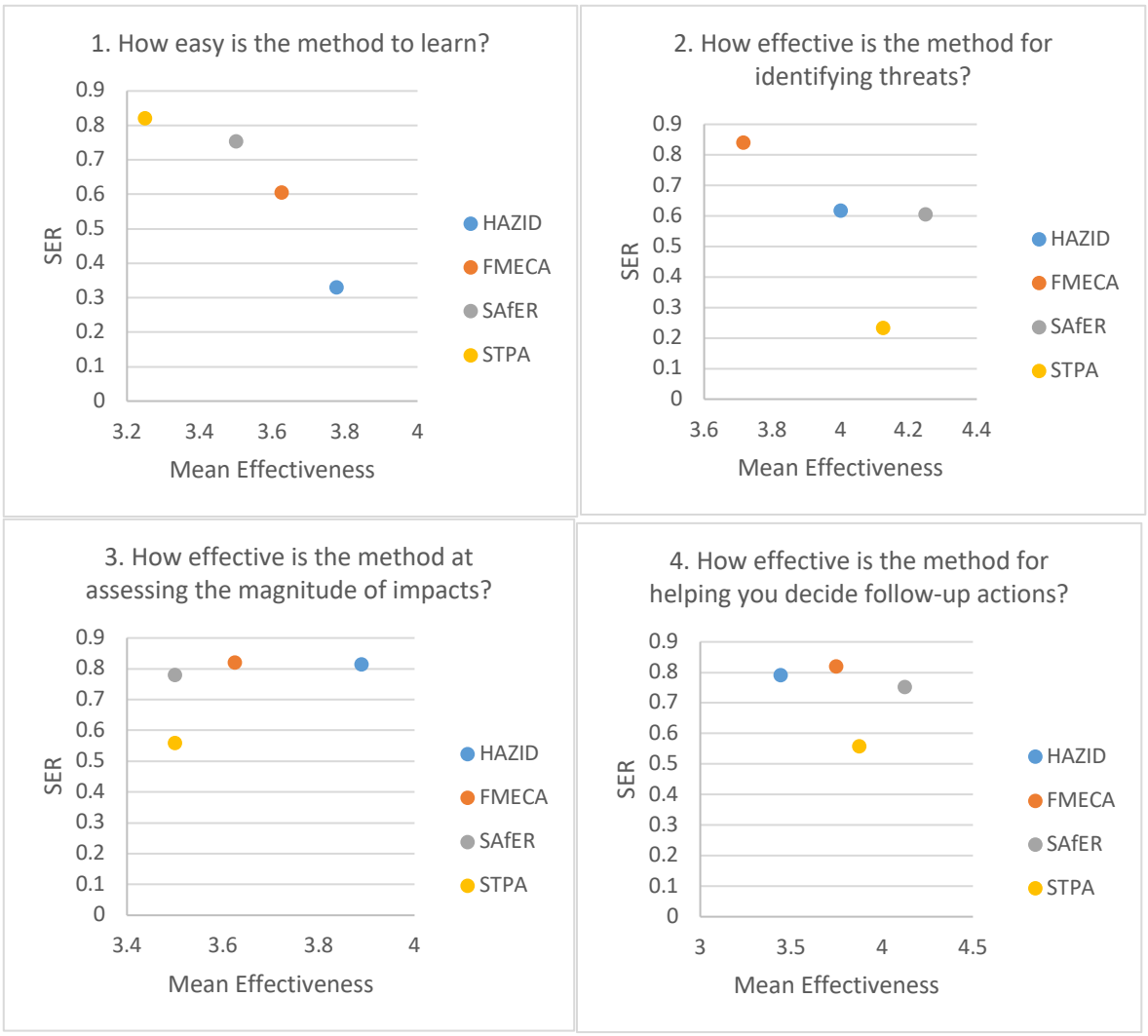


Figure A34 - SER vs Mean for each Questions 1-4 (post-workshop, longwall and process plant combined)

- Table 3 and Figure A34 should be read together.
- Identifying the 'best' method based on these survey results should be done by looking at the combination of its mean score and the SER – a measure of strength of consensus. If there is a higher consensus that a method should be that mean score, then the mean is more representative of the 'true' value of the perception of participants.
- Different methods were perceived to be useful for different purposes. HAZID was perceived as easiest to learn and best at assessing the magnitude of impacts. SAfER was perceived as best at identifying threats and deciding follow-up actions.
- On three of the four graphs in Figure A34, STPA had the second highest mean, but lowest SER. Further work should be done on a larger cohort of participants to compare the effectiveness of these different methods, and to find out the significance of the spread of the data on identifying the best method for a given context.
- These values are only part of the result of this project that should be considered, but they do suggest that perhaps, for automation systems, multiple methods could be used together to achieve best overall effective outcomes.

Questions 2, 3 and 4 of the post-workshop survey were related to some aspect of method effectiveness. Although it may be considered simplistic, being able to identify threats, estimate magnitude of impacts and help with deciding on follow up actions could be considered to be three orthogonal aspects of a more general, overall effectiveness of that method. Following this train of thought, we combined the score for each method, and both the longwall and process plant responses, into Figure A35, which is a distribution representing the overall effectiveness of each method.

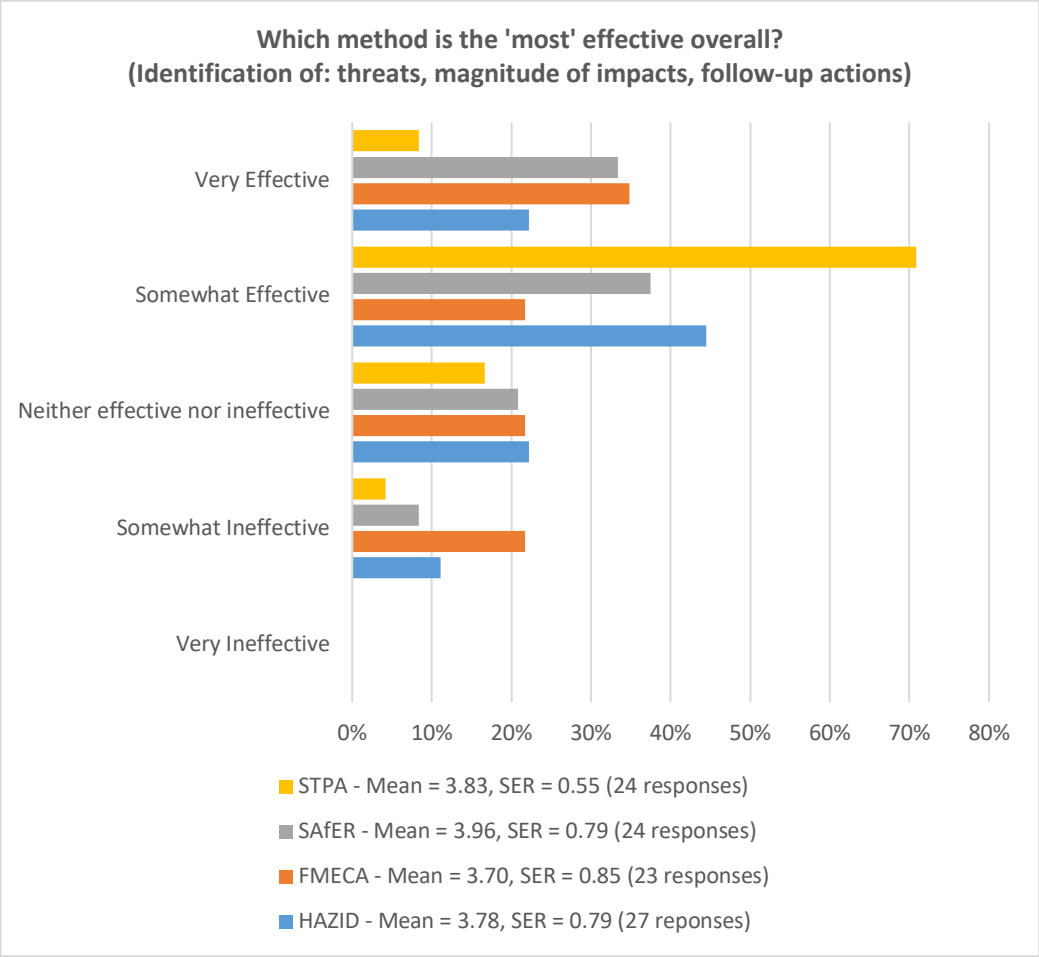


Figure A35 - Overall Effectiveness (combining responses from q 2, 3, 4 from post-workshop survey)

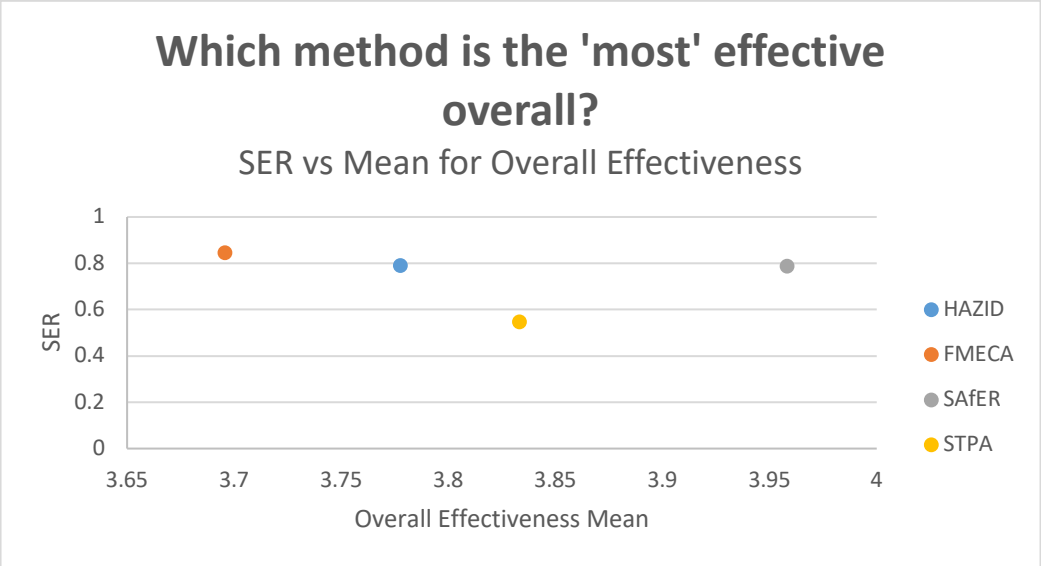


Figure A36 - Choosing the Best Method - Shannon Entropy Ratio (SER) vs Mean of Overall Effectiveness

- From Figure A35 and Figure A36, SAfER had the highest overall effectiveness score.
- SAfER had the highest mean, in terms for overall effectiveness of identifying threats, magnitude of impacts and follow up actions.
- STPA was second, then HAZID then FMEA.
- However, again, STPA had the second highest mean but lowest SER.
- All means were above 3, and so in general all participants thought that each method was generally effective.

Effectiveness is not the whole story, since ease of learning matters as well. For a method to be applied in the workplace, how easy it is to learn is a necessary enabler as well as its actually effectiveness. These two factors (Overall Effectiveness and Ease of Learning) are the two key features to compare these risk assessments methods. Figure A37 shows the comparison between these two variables.

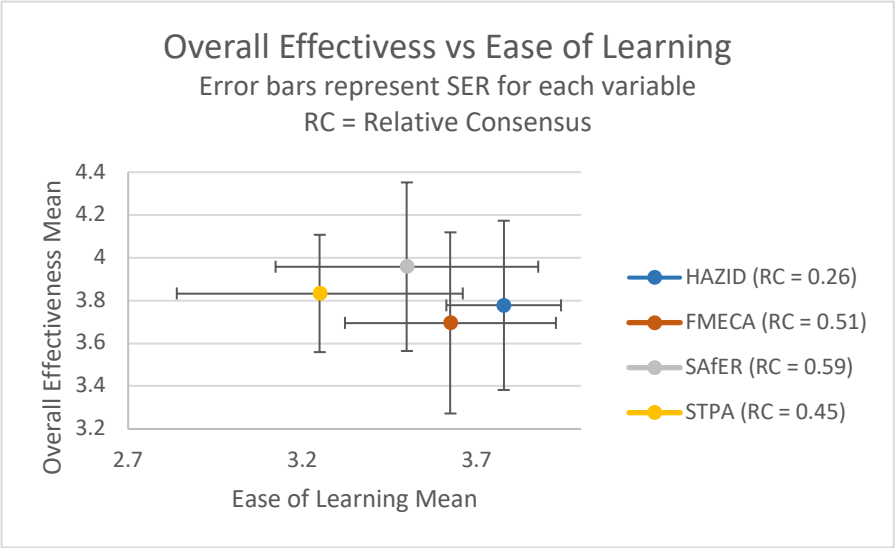


Figure A37 - Comparison of Overall Effectiveness and Ease of Learning for each method

Error bars represent Shannon Entropy Ratio (SER) for "Ease of learning" and "Overall Effectiveness" respectively. The SER represents the consensus for each of these variables - how close or how far from a uniform distribution (no consensus) the results for each method were. The 'area' represented by the combination of both error bars is in indication of the combined consensus about that method over the two key variables: ease of learning and overall effectiveness. Multiplying the SER scores for these two variables gives a 'relative consensus' overall for each method – a representation of this area, as shown in Table 4.

Table 4 - Comparing Ease of Use with Overall Effectiveness, noting Relative Consensus

Method	Mean 'Ease of Learning	Mean "Overall Effectiveness"	Relative Concensus (RC) (SER_ease*SER_Effectiveness)
HAZID	3.78	3.78	0.26
FMECA	3.63	3.70	0.51
SAfER	3.5	3.96	0.59
STPA	3.25	3.83	0.45

- If we treat effectiveness and ease of learning as equivalently important for a moment, it is plain to see that SAfER and HAZID are both the best, as in Figure A37. HAZID for being easiest to learn, and SAfER having the highest overall effectiveness. However, SAfER had the highest RC (area of the error-bar-square around its mean) and HAZID the lowest.
- HAZID has the lowest SER for Easy of learning, and STPA has the lowest SER for overall effectiveness.
- The fact that the 'area' boxes in Figure A37 overlap is not meaningful in this context, since the error bars don't represent the range of the data, but the SER.

2 Pre and Post Workshop Comparison of Free-Text Comments

Table 5 – Comments from Pre and Post Workshop Surveys on all methods

Pre/ Post	Method	Comments	Workshop
PRE	HAZID	Common method regularly used in mining. Allows a broad scope to be considered of equipment, process and behavioural factors. Facilitation is very important (as is most methods). Does not always result in a comprehensive assessment.	HAULAGE
		HAZID usually relies on experience or past performance which is difficult with a new technology and processes	
		Used similar tools	LONGWALL
		A good technique to use	
		no	PROCESS PLANT
		I haven't used it before cannot really comment at this stage	
		Heavily reliant on facilitation and knowledge of the topic.	
	FMECA	It does not show the layers of protection that is typically built into an autonomous system. It does not seem to require a good knowledge of how the system SHOULD work; difficult to keep to human factors only.	HAULAGE

		The elements of human/system risk do not fit well with the component >function approach of the FMECA template. Technique probably demands more time to get results than HAZID	
		Appeared to really open up and could see getting lost in volume without getting to specific issues/risks/controls	
		was difficult not to consider layer of protection	
		FMECA isn't well suited to high level design	
		FMECAs can become very large and complex, making it difficult for people to comprehend	LONGWALL
		In my experience FMECA is slightly miss-aligned to this scope.	PROCESS PLANT
		There is no appropriate response for 4 onward if you have not completed this type of risk assessment for	
		Happy with the results I get with this technique	
	SAfER	Appears to be good to identify improvements and practical ideas to become safer. It is positive (inspiring) but don't get bogged down in 55rying to assign numbers; avoids the admin control trap (ditto for training – a cop out). It highlights the fact that we can design out the human mistakes	HAULAGE
		A good introduction to a new approach. Likely to challenge designers more than operators. Greater flexibility than traditional methods.	
		Generally engineering controls are longer and more difficult to implement	
		Not really ranking risk? Prioritise?? Speed of decision? Design document	
		System design tool focussed on safety strategies>>not really a risk assessment	
		never used before	LONGWALL
		questions 4,5,6,7 hard to answer as I have not used this technique before	
		Have not used this technique before	
		Brief introduction to this method associated with the UQ study in progress.	PROCESS PLANT
		Haven't used it before	
	STPA	Good in that it focuses on control system and human interface but does not account for the LAYERS of protection	HAULAGE
		Looks to be useful in helping a group to better understand the complexity of a human >control system. Feel lit could be time consuming to fo thoroughly. The risks and controls development process is not too different to other techniques.	
		The mapping of the process appears to aid in identifying issues. Appears to look like it would be helpful in specific narrow scope aspect to RA.	
		I would consider using following HAZID to expand on scenarios.	
		I would use this to conduct a deep dive on identified high risk scenarios	
		Unable to answer 4 5 6 7 as i have not used this before today	LONGWALL
		Have not used technique before	
		-	PROCESS PLANT
POST	HAZID	Good technique to use	
		I can see it being difficult to distinguish/evaluate the difference in risk between remote operations vs on face operations	LONGWALL
		I think it is very subjective	PROCESS PLANT
		Does not specifically assist with targeting human- system interactions. As people are familiar with this method the outcome is still reasonable.	
		Quality limited to the people attending the risk assessment	
	FMECA	Good technique, does go into detail - a little more challenging than a standard RA	LONGWALL

		I think a process based FMEA or FMEA with human factors (see table F.13 of AS60812) may work better	
		FMECA is very effective a tool in determining corrective actions	PROCESS PLANT
		this technique seems like it would work better when used in more specific situations rather than at higher level risk management	
		In my experience this method is better suited to detailed equipment failure analysis to determine maintenance requirements rather than human - system risks.	
	SAfER	Safer was a good tool to use alongside a RA or equivalent ?>	LONGWALL
		a little hard to get my head around the first section in regards to plant operation but i think the second part is useful to help understand how someone may react in different situations	PROCESS PLANT
		Not as simply in application in comparison to other techniques	
		Not as familiar with this methodology, however it appears to be more human focussed.	
	STPA	The process model is a good tool to visualise	LONGWALL
		A good technique used in combination with an RA	
		Flowcharting part of STPA appears useful - particularly for communicating to operator/trades	
		The development of the graphical representation of the control elements is a good way to get alignment with the RA team.	PROCESS PLANT
		Cannot be carried out without knowledge of the control systems	

From Table 5, we have identified key factors for helping analysts choose a method for performing hazard identification and risk assessment for systems containing people and autonomous systems interacting. That is, consider the following factors when selecting a method:

- Scope.
    - HAZID suited to broad, less detailed scope for risk assessment.
    - FMECA, SAfER and STPA all were thought to be more applicable to narrower, more detailed scopes. For example:
        - FMECA useful for equipment failures
        - STPA useful for exploring control systems and ineffective control scenarios
        - SAfER useful for understanding and describing how and why people make decisions.
- Ease of use.
    - HAZID was the easiest to use, and the method most participants were familiar with.
    - FMECA/SAfER/STPA were more difficult to use, across the workshops, but yield more detailed results from narrower scopes.
- All methods require facilitation. This is perhaps an obvious point, but it is a key factor often identified for enabling the successful use of a risk assessment method.
- Combination of Methods. Participants mentioned a few times that combining methods, or parts of them, together could be more helpful than using one by itself. For example:
    - Using a risk analysis for decision making around hazards combined with STPA to look at control failures and their contribution to hazard exposure.
    - Exploring both control system dysfunctional interactions and more localised equipment failures.
- Process for the analysis team to go through. Different methods took participants through different kinds of group processes. Choosing what kind of group process organisations may

want their risk assessment teams to experience can affect the functionality of the team and the outcomes of their analysis. For example:

- HAZID – it's less structured than the other method in terms of *how* to go about identifying hazards/controls. It just said you should do that, not how. Some relevant quote include: "It's very subjective"; "Relies on past experience". That is, HAZID is a facilitated discussion around system hazards, with less detailed system decomposition and analysis.
- FMECA – Equipment failure analysis. A more structured analysis than HAZID. That is, you're focussing the risk assessment team more on one key issue. A different group process than HAZID.
- STPA – This is more like design thinking, since you have to build a control structure **together**. You're producing an artefact together (control structure). This is a different group process than HAZID or FMECA, and emphasise team building and deeper alignment. Relevant quote about STPA: "*The development of the graphical representation of the control elements is a good way* ***to get alignment with the RA team.****"*
- SAfER – Being quite a different kind of method from those normally employed in the mining industry for risk assessment, SAfER can **challenge** design teams with getting them to really think about how the operators make decisions, and how to enable better outcomes. Relevant quote: "*Likely to challenge designers more than operators".*

3 Conclusions and Future Work

Combining the results of the question analysis with that extract from the free-text comments in Table 5, the following are the key conclusions from this analysis:

- Using multiple methods in systems with automation may well be advantageous. For example, note the comments regarding Figure A34. HAZID is easy to use, and perceived as most useful for identifying threats. SAfER was perceived as the most effective for identifying magnitude of impacts and suggesting follow-up actions. SAfER also had the highest overall effectiveness. However, since the SER for STPA was consistently lower than the other methods, it may well be that SAfER's dominance these areas of effectiveness may well not stand up to further experiments, and as more data is gained STPA may indeed be the preferred method. Additionally, from the comments in Table 3, HAZID is useful for broader scopes and lower required detail, whereas FMECA, STPA and SAfER are naturally narrower in scope but can support a more detailed focus analysis in a particular area: equipment failure, control system design holes and human decision strategies. Different methods are useful for different purposes, and for systems with automation and the diversity of issues, functions and failures they can experience, using a combination of different methods could be the best way forward. It may turn out that only parts of each method may need to be combined with parts of another, rather that perform two or more full analyses. Exploring this more fully should be a key focus of future work.
- The SER score is useful for identifying the most effective method, given a particular survey question. But it is only a clue. Low SER is a clue, not hard evidence, that a method is well understood and has clear consensus for a particular purpose. For example, quite a number of times, STPA had the second highest mean, but lowest SER. Further work should be done on a larger cohort of participants to compare the effectiveness of these different methods,

and to find out the significance of the spread of the data on identifying the best method for a given context.

Appendix B: Case Study Information

Scope for autonomous surface haulage

The scope used for the automated surface haulage case study is shown diagrammatically in Figures B1 and B2 and is described in more detail in the scope table shown in Table B1)

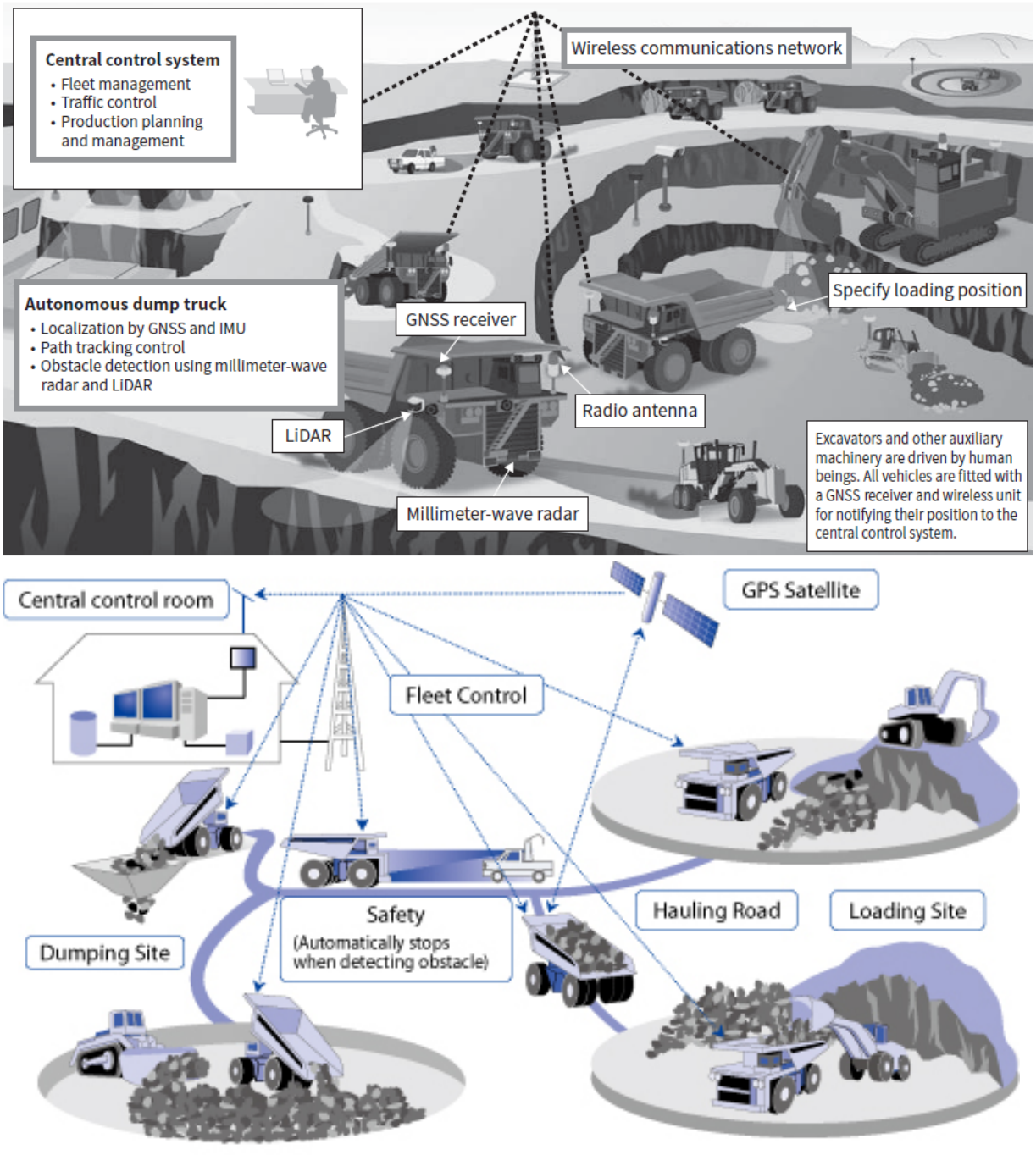


Figure B1: Overviews of autonomous haulage systems (sourced from https://www.hitachi.com/rev/archive/2018/r2018_01/pdf/P087-092_R1a07.pdf and https://home.komatsu/en/company/tech-innovation/solution/)

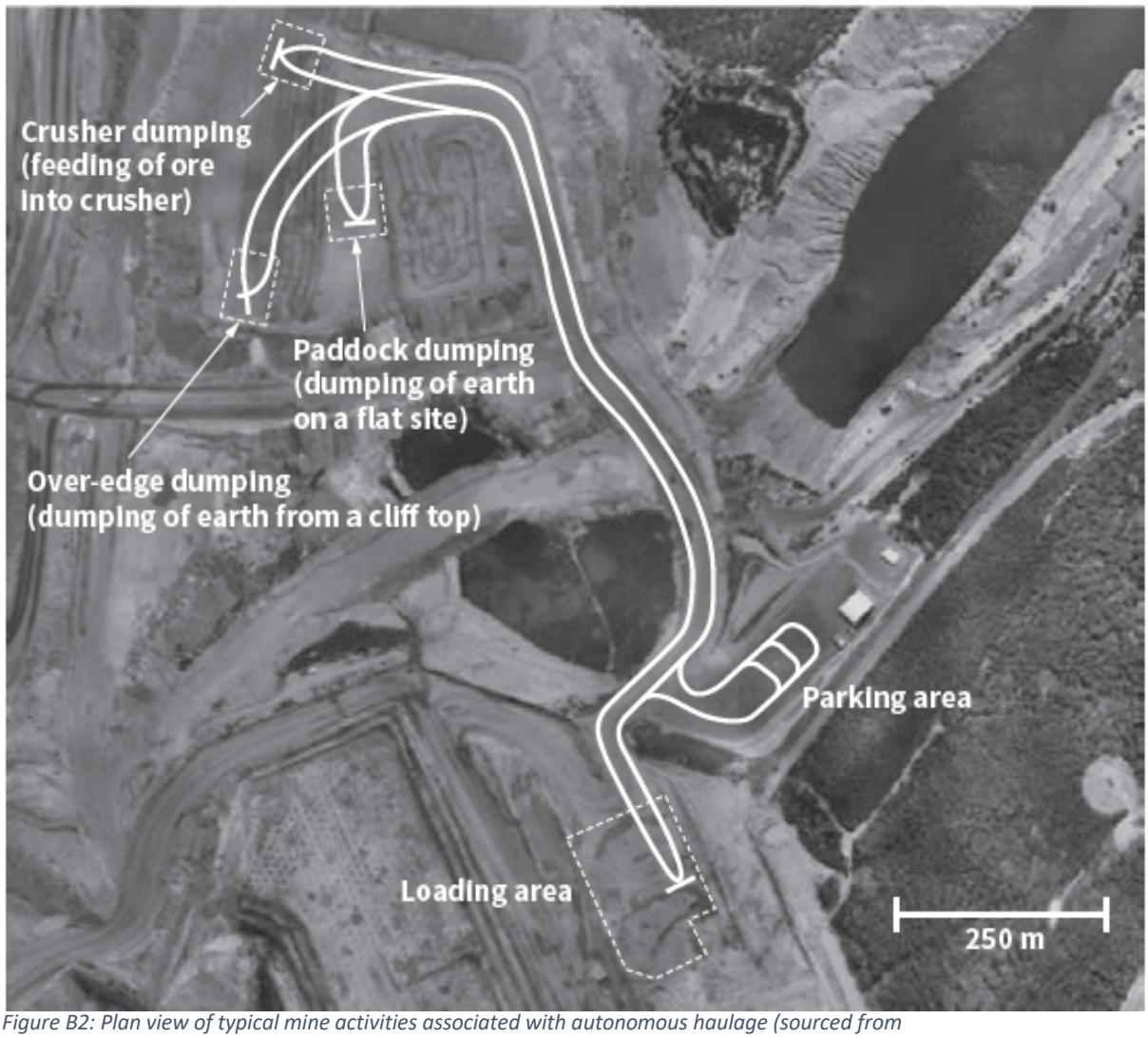


Figure B2: Plan view of typical mine activities associated with autonomous haulage (sourced from https://www.hitachi.com/rev/archive/2018/r2018_01/pdf/P087-092_R1a07.pdf)

Table B6: Autonomous Surface Haulage Risk Assessment Scope

Attribute of scope	Included	Excluded
P: People involved in risk management or potential impacted if risks are not managed	Employees, contractors, OEM personnel and visitors accessing automated haulage areas and/or equipment. Roles include - Controllers who manage automated fleet - People who are in charge of maintaining the virtual map of the mine - Controllers who manage other/manual pit operations - Pit personnel who operate manned mining and ancillary equipment - Autonomous vehicle field support - Manned vehicle field support - Other personnel that enter into pit (e.g. supervisors, geotechnical, mining and other technical specialists, etc) - IT & communications people - Vehicle maintenance people Visitors – authorised and unauthorised	People outside the autonomous areas in the pit and outside the pit control rooms.
L: Locations or areas where the risk exist or that could be impacted if the risk event materialised	Surface lease areas accessible to automated fleet (operating in autonomous/semi-autonomous modes) - Roads - Active mining areas – including loading, hauling and dumping area - Park up areas and zones where trucks transition from autonomous to manned - Refueling areas	Off-active lease areas including exploration Care and maintenance sites Onsite fleet and tyre workshop areas and new equipment delivery and commissioning areas
E: Equipment and plant (e.g. tools, vehicles, fixed processing plant, infrastructure etc)	Autonomous haul trucks Load units (manually driven) Water carts (manually driven or autonomous) Road maintenance equipment (manually driven) Load and dump area cleanup plant and equipment Vehicles that fuel and service in-pit equipment BOMB/MMU/MPU truck Other ancillary equipment (e.g. lighting towers, communications and network hardware etc) Light vehicle fleet	Aerial vehicles (manned and unmanned). Other stationary in-pit equipment eg sumps/pumps, crushers and conveyors. Process plant area

A: Activities (e.g. operations, maintenance, startups etc)	Loading, hauling, dumping, in-field troubleshooting, equipment cleaning, roads and other work areas where automated haulage equipment can access. Human-system interactions include: - Manual digging and loading of trucks - Shift and break changes for dig, dozing and cleanup equipment operators - Manual inspecting, mapping and surveying of mine involving people in light vehicles and on foot - Haul road watering involving manned vehicles or automonous - Haul road maintenance involving manned vehicles - Hauling and dumping at ROM, berms (manual/auto), paddocks, over-edge both in autonomous and manual modes - Cleanup around load, roads and dump areas performed by manually driven equipment - In-pit manual intervention to inspect, troubleshoot and/or reset autonomous trucks includes people on foot approaching trucks - Queuing of vehicles at loading and dumping areas - Refueling of vehicles – both manual and autonomous - In-field servicing of vehicles – both manual and autonomous - Parkup of vehicle – both manned and autonomous at active mining areas, on haul roads, at cribs, workshops etc - Accessing autonomous equipment – in-field - Transitioning autonomous equipment from manned to automated mode and vice versa - Control room oversight of autonomous fleet - Mine control of entire operations including authorising entry, dispatching, allocating water truck and ancillary fleet duties etc.	Delivery, unloading and commissioning of new vehicles. Decommissioning and removal/disposal of old/written-off vehicles. Areas outside autonomous zones e.g. Drill and blast areas. Rehabilitation activities
T: Timeframe (e.g. time based exposure info, timezone info and how far into the future)	Continuous operation – 24 hours per day, 7 days a week, all seasons of the year in Australian climatic conditions. Consideration should include shift and break changeover processes Adverse climate conditions – wet weather, lightning, dust, fog, ice, and extreme heat/high temperatures.	
S: Known risk scenarios that need to considered	Potentially fatality or severe injury resulting from unsafe human-automation interaction associated with: 1. Manual and autonomous driven vehicles operating in same area includes manned light, ancillary and heavy fleet operating where autonomous haul truck are operating includes • Ensuring digital maps accurate reflect the actual/live/current status of the physical operational area • Operators setting accurate assignments from field – bays, spot points etc for autonomous vehicles • People understand where automated zones exist and different zones within automated area	Autonomous vehicle fire. Autonomous vehicle – autonomous vehicle collision Manned vehicles incidents not involving autonomous vehicles Interactions with automated water trucks – future scenario

	• People understanding what the autonomous vehicle status and intention 2. People parking light vehicles and being on foot in areas where autonomous trucks are operating includes: • People performing normal mine duties e.g. installing signage, operator change-outs, vehicle maintenance & refuelling • People approaching and moving away from autonomous haul trucks that has stopped/broken down in the field. • People approaching and moving away for vehicles transitioning trucks between manned and autonomous mode in designated area 3. Human responding/not responding to control system guidance, safety alerts and exceptions • Operators remote controlling from the field • Control room controllers overriding control system or misinterpreting/incorrectly handling exceptions • Control room controllers setting assignments from control room – bays, spot points etc for autonomous vehicles	Interactions with automated dozers – future scenarios

The potential future risk scenarios that could be considered are:

- Introduction of autonomous water trucks/carts
    - Under, over, correct watering impact on human-system interactions
    - Changes to interaction risks – deciding mission, truck filling up processes (parking & refilling)
    - Impact on functionality – fire fighting, truck washing, excavator walking etc

The high risk activities for decomposition are as follows and the decomposition is shown in Table B3.

Table B7: Functional Decomposition of risky AHS interactions

Interaction	Description of functions to consider	Comments/Issues to consider
Manual and autonomous driven vehicles operating in same area includes manned light, ancillary and heavy fleet operating where autonomous haul truck are operating includes - Ensuring accurate digital maps and that people understand where automated zones exist and different zones within automated area	1. Autonomous and manned trucks travel on haul roads includes interactions with - water truck - explosive truck - road maintenance vehicles (working vs traveling / impact on overtaking) and personnel - light vehicles - fuel and service trucks - interaction with spillage (e.g. hit rock which turned into a projectile) 2. Autonomous and manned haul trucks queue while wait until called into position by load unit, then manoeuvre into loading position, then leave when dispatched/kicked out by loader includes - load unit operator setting spot position and taking control of truck if positioning needs correcting - interacting with clean up machines 3. Autonomous and manned truck dumps load at dump station (e.g. ROM) in autonomous mode 4. Autonomous and manned trucks transport waste to tip head or waste dump, manoeuvre into position, dump load then leave includes - interacting with dozer - dozer operator setting dump position 5. Refueling of haul trucks in field and at fixed refueling station	• Accuracy of digital maps • People understand where automated zones exist and different zones within automated area • People understanding which equipment is operating in automated mode and which equipment is manned • Intersection changes (e.g. adding slip roads) and rule changes can cause issues for manned vehicles • Changes in haulage routes can cause issues if operators “follow haul truck tire marks” rather than screen information – related to trucks intention and whether trucks are behaving as they should.

Interaction	Description of functions to consider	Comments/Issues to consider
People parking light vehicles and being on foot in areas where autonomous trucks are operating includes: - People performing normal mine duties e.g. installing signage - People approaching and moving away from autonomous haul trucks that has stopped/broken down in the field. - People transitioning trucks between manned and autonomous mode in designated area	People on foot required to have vehicle with protection bubble and they are required to create a lock out area (exclusion zone that can't be changed in field or lock out zone created by operator through screen) before exiting vehicle. They need someone watching over them or have a portable R-stop. Not allowing people to be on foot in same work area where autonomous vehicles are operating. Swap out of operators occurs after the operating area is locked out. Control room provide oversight monitoring of compliance. To approach truck – truck needs to be stationary. - If in known parking area, the area will the locked and truck is shutdown remoted (engine stopped and brakes are applied) – there is no boarding of an AT when engine is running. - If in field – the truck still needs to be stationary then area locked then engine shutdown using remote control. Additional lights are on front of truck to confirmed engine shutdown and brakes applied (unique to ATs). If out on ground there needs to be a lockout & MIV = manned instrumented vehicle = vehicle equipped to do locking. Should not lock area then have vehicle leave. Exceptions are special areas like the transition area, in these cases they need R-stop and positive communications with control room. # AT stopped/parked on inclines are not considered to be parked in a fundamentally stable manner so they undergo risk assessment before recovery because have to approach on foot to recover it. # Differences between OEMs about protection "bubbles"/"lockouts" # Humans can find/assume AH are highly predictably when in autonomous mode which can lead them to be less cautious. # There's a challenge knowing where the lockout is with respect to the physical ground – can see in on HMI in vehicle but not when on foot so wondering outside locked area is a real risk.	• Humans need to "logon" to be recognised by haul truck. • Humans can leave vehicles to do inspections etc and still consider they are protected by vehicle "bubble".

Interaction	Description of functions to consider	Comments/Issues to consider
Controllers overriding system guidance/safety features and understanding and responding to exceptions	Controllers don't have situation awareness so are relying on communication from others in the field to make decisions around permissibility of actions. Override done when truck has detected something and stopped in field - Need operator to check for obstacle and communicate back to control room that it's safe/unsafe to proceed. - Risk of becoming complacent if lots of false stops - Once truck are overridden they will travel some distance before detection systems fully functional – operator may not be aware of clearances limits requirements - Only takes one operator to give approval to override – sometimes have more than one operator in area – so could approve override while someone enters area. - Could have multiple trucks that are stopped and there is potential that wrong one is reset/overridden - Different function for resetting from MIV versus control room Control room operators distracted/overloaded/experience alarm flood and knowing right sequence and respond to execute to action alarms. Have special overrides that require special codes – e.g. resuming operations from an all-stop.	
Introduction of autonomous water carts	Management of autonomous vehicle interactions will be as per above mentioned scenarios The autonomous management of the road wetting/spraying process needs to be evaluated in terms of • Impact of overwatering causing a loss of traction or even water pooling that triggers sensors • Impact of underwatering causing dusting issues that impact on line of sight and sensor systems	

Assumptions and Caveats

For the purpose of the Automated Haulage system human-system interaction risk assessment it is important to note the following assumptions were made

- All automated haul trucks are fitted with similar layers of protection, regardless of the technology provider, and these include
    - Proximity detection and collision avoidance systems to protect vehicle from obstacles while travelling forward and backward
    -
- All loading will be conducted by manually driven equipment
- Clean up around loads and dumps will be conducted with one or two manually driven equipment per area

HAZID results for autonomous surface haulage

The first risk assessment technique undertaken was the HAZID analysis. The results of this analysis are tabulated in Table B4 which shows the relevant information from the full HAZID spreadsheet. The hazard column listed mechanical so it has been excluded from the table. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table B8: HAZID analysis for Autonomous Surface Haulage

Description of unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis: Estimate of Likelihood	Risk analysis: Overall Risk Rank
Person approaches truck and truck moves off = Unexpected movement of autonomous truck	After recovering from exception - in most cases truck moves some distance before it recognises obstacles again	Plausible fatality if person is in line of fire	5			Catastrophic	Unlikely	Very High
	Control room gives truck permission - could be because the control has mixed messages from another field person							
	Operator fail to isolate/suspend truck before approaching							
	Operator doesn't carry A-stop (CAT)							
	Operator not following procedures for approaching truck (e.g. lack of training, shortcutting, complacency)							
	Park-brake failure - it may not be on level ground or parked fundamentally stable fashion							
	Obstacle detection system on truck not detecting person							
Manned vehicles (site aware vehicles) coming in close proximity of AHT vehicle and vehicles collide	Operators ignoring alarms/ alerts	Vehicles make contact - likely fatality, in some scenarios could be multiple fatality	5			Catastrophic	Possible	Very High
	Trucks not being able to brake in time							
	Obstacle detection system on truck not detecting vehicle							
	Hardware/comms system failure/malfunction							
	Slippery ground conditions							
	Unauthorised equipment entering site (not site aware vehicle)							
	Over-reliance of system (e.g. parking too close because "know" system will stop vehicle)							
	AHT under remote control of digger/dozer. Could remote control them into another vehicle							
	Controllers not watching screen so they don't react in time to prevent collision							
	Manual vehicle not paying attention and u-turn in front of autonomous vehicle							
	Forgetting trucks are autonomous and not focusing on what you are doing around them							

Analysis results are only examples, done to demonstrate how this part of spreadsheet works. Risk analysis should be done when the specific context is known

Description of unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis	
							Estimate of Likelihood	Overall Risk Rank
Control room operator overrides control system when it should not have been - Important to note that depends on the nature of the override	Pressure placed on the CRO to do so	Autonomous vehicle collision, resulting in asset damage and stopped operations - most plausible. Could also lead to AHT colliding with manned vehicles but less plausible	5			Catastrophic	Unlikely	Very High
	Loss of situation awareness of what is happening in the field							
	Incompatible situation awareness between control room and the field							
	Incorrect operator permissions - person may not have training/quals for the things that they have access to							
	Training lags changes in system functionality so person might not know whats required							
	System is not real representation of the world - presents the wrong information - Virtual mine doesn't match physical world	Doesn't pick up obstacle (e.g. light plant), could lose asset (e.g. over dump, rollover)						
Unauthorised access - e.g. boom gate overrides let vehicle into autonomous zone	Boom gate overrides let vehicle into autonomous zone	Multiple fatality = potentially a number of people in vehicle not knowing its autonomous zone and without required controls	5			Catastrophic	Possible	Very High
	Incomplete training/ knowledge of what is required							
	Following a vehicle through boomgate							
	Breach in the perimeter - away from the boomgate							

FMECA results for autonomous surface haulage

The second risk assessment technique undertaken was the FMECA analysis. The results of this analysis are tabulated in Table B5. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table B9: FMECA analysis for automated haulage

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
Site aware vehicle	Monitoring position on screen	Too infrequently checking. Looking too much at the screen. Loss of power - e.g. due to bumping switch. Ambient light/scratches/ dust makes hard to see. Confusing information - not easy to see at glance Lag on the screen. Not centred on your part of the mine. Operator doesn't act on information provided	Interface design issues Takes too long to read/understand information Robustness issues of design for different user preferences	Get in the way of a haul truck which stops = disrupts production Collision between AHT and site aware vehicles	5					
	Pausing a truck (touch truck then pause) or Suspending truck (shut down to safe space = virtual lockout). Symbol and colour of truck changes on screen and mode light on truck changes when it is done	Not doing it, select wrong truck (if control selects wrong truck), communication loss,	Communication loss. Miss communication about right truck. Education/ training	Might pause to try and clear work area = if couldn't pause could cause asset damage						
	Protect occupant - inside and outside vehicle within bubble	Unauthorised vehicle that doesn't have control, incorrectly selected mode, wander outside bubble, failed to create locked area, failed to follow procedure, don't know what area is locked, don't lock out area with your lock because it is already locked	Education/ training, failure to report location/ position of vehicle, shortcut, procedural breach, loss in situation awareness/ concentration, possible you think you have locked out and already locked area but haven't, in a shadow area where R-stop not effective	Catastrophic - potential that person(s) will get run over						

Did not complete this section as it was not part of the workshop. Risk analysis should be done when the specific context is known

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
	Communicate position to central system	Comms or GNSS failure, giving incorrect position, system turned off	Fault, incorrectly fitted/ maintained components	System health checking process shuts trucks down = throws bubble Control room operator cannot see vehicle in field						
	Surveying road conditions	Incorrect survey locations, not surveying windrows, map built incorrect to survey locations	Education/ training	Truck might fault if obstacle detection working else it could go through windrow, over the edge (and possible into another vehicle below)						
	Escorting unaware equipment	Escorted vehicle moves outside protection bubble, left escorter alone, vehicle turns bubble off before escort finished	Poor communication between escort vehicle and escorted vehicle, training/ education	Catastrophic if light vehicle driving around undetected, could be collision with truck						
	Creating spot points / bays - done by load unit operator on the screen, any MIV can create point/bay on dump	Failure to create bay, bay is in incorrect position	Training/ education, interface was not sufficiently designed for easy/accurate/efficient use	Truck wouldn't move if no bay, or could dump in wrong place truck or could go over edge but cant put bay outside map, edge protection controls and inbuilt sensors						
	Restarting a AHT truck - after it has gone into stop due to obstacle / exception, includes reviewing and clearing errors and exceptions	Having actual world not aligned to virtual world - not aware of obstacle (berm, light plant) being near truck. Not seeing or communicating obstacle	Incorrect actions taken when trying to start truck. Miscommunication about which truck to start	In most cases the truck will fail to safe so effect is production loss (because truck is down and/or causes other trucks to queue/stop). If wrong						

Component Name	Component Function	Failure Mode(s)		...re	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
		that stop truck. Restarting wrong truck		...the ...row						
	Validating virtual model	Bay is in incorrect position								
	Transition truck from manned to autonomous	If not set up right you can start it but wont go to autonomous								
	Providing visual map on screen of virtual system									
	Check of AHT equipment on system - health check, any alarms									
	Emergency stop of system									
	Dispatching of AHTs - call up and kick out AHTs from loading unit									

Not completed in workshop due to time constraints

SAfER results for autonomous surface haulage

The third risk assessment technique undertaken was the SAfER analysis. The results of the situation assess part of the SAfER analysis are tabulated in Table B6. The results from the strategies analysis part of SAfER are shown in Table B7.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

Table B10: Situation assessment part of SAfER analysis

Situation Assessment Indicators	List the indicators that need to be monitored to check for safe/unsafe operation?	What design improvements could make these indicates easy to perceive, comprehend and project into the future?
Plant/process factors	If the autonomous area is active or is inactive e.g. boom gates up/down, status board and lights If there is an active R-stop within reach Is interface in equipment fully functioning and logged in and working Status = Presence/Absence of critical alarms = alarms for which action needs to be taken e.g. non-authorised asset in autonomous zone, flashing tiles on the system Mode that the AHT in = autonomous, faulted, manual Intended paths and permissions of AHT Which area(s) have been locked out - can see on screen but challenging to relate that to where it is on the ground in real world If safety bubble is required and is present Two-way communication system working	- Boom gates that can only be controlled by one person. Boom gate interlocked to system so it would only open if safe for person to attend. - Illumination that shows health status of R-stop, tracking of portable R-stop that interlocked with boom gate so not allowed in unless have active, healthy e-stop. Interface functionaly included with boom gate interlock. Interface design to right detail and coverage for different operations. Improve radio so not overloaded - especially with control room operator - find a way to communicate the comms load on the operator (e.g. number queued waiting for response). Move from verbal comms to message system via interface or press button for routine acknowledgement. Some way to convey lockout area boundaries to ground in real world e.g. lazer on ground or AR safety glasses or audible beeper/voice
People factors	Authorised, trained people and tasks that they are appointed to. Tracking of people/assets in/out of autonomous zone - don't need to monitor in certain circumstances	Linking of training and badging in/out system so only authorised people can enter through boom gates
Context factors	The boundaries of the autonomous zone is clear to those working inside and outside of zone - so those operating outside don't inadvertently breach autonomous zone Is interface lining up with what is happening in real world - need to monitor mine survey area aligns with virtual area The road conditions - and that the autonomous vehicle speed is adjusted to suit road conditions. Loading and dumping method used - and that the autonomous vehicles are set according to these methods	- Windrow and signage as well as digital boundary proximity monitoring and alarms (spoke voice explaining risk) on all fleet onsite

Table B11: Strategies analysis part of SAfER (blue is normal operations, purple is abnormal operations)

Generic Strategy Prompts	**What plausible decision/actions related to this generic strategy could be used in the system being analysed?** (Consider examples for both normal and abnormal operations)	**What consequences might result if people adopt this strategy?**	**Should design promote, prevent or tolerate strategy?**	**What design improvements would improve response strategies during normal, abnormal and unexpected situations?**
Avoidance = Not done, defer, or forget to do	Entering without portable R-Stop when intending to get out and move away from vehicle	Unable to emergency stop the fleet from your location	Prevent	Personnel tracking to show positioning with respect to R-stop
	Entering without an active R-Stop	Unable to emergency stop the fleet from your location	Prevent	Boom gate interlocked doesn't open unless R-stop active
Intuitive = automatic response, done without explicitly or deliberately using thought processes	Light vehicle drivers take pathways through corners to avoid projected permission trajectories avoid recoveries - info is on screen but after time don't need to look at screen to do	Prevents trucks stopping and having to be recovered	Promote	
	Parking in line of fire expecting controls to prevent collision	Collision if controls fail	Prevent	Not park in wheel tracks - needs further thought. At present relying on locking system out
Arbitrary-choice = guessed, scrambled haphazard or panicked response	Have to guess when permission line hasn't quite reached your area so have to guess whether to go or wait for the permission line to reach you	Slow down production because truck detects you in permission will slow down	Tolerate	Design variable is how much permission that ask for in front = how much distance they can stop safely within. Instantaneous and continuous permission or countdown when permission will be give. Have a request line in front of permission line. Can have and use special rules for special areas. Hard for system to be fully flexible and not end in deadlock
	Have to guess where sighted vehicle bubble extends to	Could venture outside bubble protection	Prevent	Personnel on foot to be provided with individual bubble protection
Imitation strategies = copy how others do it or copy what has worked in the past	Assume trucks are following same path as shown with wheel tracks	Trucks could change path = collision	Prevent	
Cue-based strategies = select Chosen Option using the Observed Info/Cues and Predict Consequences results				

Incomplete due to workshop time constraints

Compliance-based strategies = following procedures as they are written/practiced				
Analytical Reasoning strategies = using analytical thinking to reason out the best way to perform task				

STPA results for autonomous surface haulage

The fourth risk assessment technique undertaken was the STPA analysis. The results of the control diagram are shown in Figure B3. The results from the risk identification part of STPA analysis is shown in Table B8.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

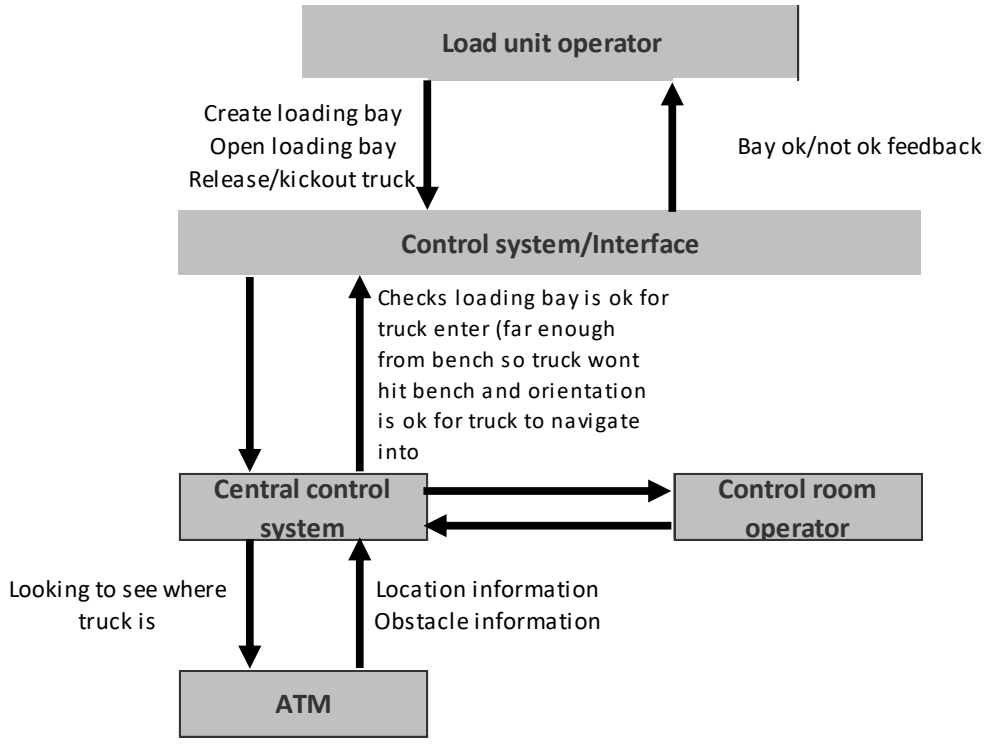


Figure B3: Human system interaction control diagram

Table B12: STPA analysis for autonomous haulage

Control action	Control Action NOT GIVEN	INCORRECT Control Action IS GIVEN	Control Action GIVEN AT WRONG TIME - TOO SOON/EARLY	Control Action GIVEN AT WRONG TIME - TOO LATE	Control Action GIVEN IN WRONG ORDER or FOR WRONG DURATION	Potential Consequence(s) and Significance (High priority - must address, Med priority - should address, Low priority - monitor for change, Negligable - No further action required)	Possible causes of unsafe control action	Assessment and recommendation for improving design (ISD) or controls or control systems (DiD)
Operator starts filling process using system "start" button	Operation doesn't execute start fill button on filling station computer	Operator selects stop (not start) filling in computer	Operator executes start command much too early	Operator executes start command much too late	Not applicable	Significant unsafe action = If started too soon, tanker may not be properly parked, connected and earthed which could lead to loss of containment and/or the intro of an ignition source making fire and explosion possible >> HIGH PRIORITY	Operator distraction or lack of competency, poor shift handover.	Install interlocks of forcing function based checklist that requires a specific operator to check system and tanker is correctly set up prior to pressing start.
Operator stops filling process using system "stop" button	Operator doesn't execute stop fill button on filling station computer	Operator selects start (not stop) filling in computer	Operator executes stop command much too early	Operator executes stop command much too late	Not applicable	Significant unsafe action = If not stopped or stopped too late then this could lead to loss of containment due to overfilling tanker which could cause fire and explosion >> HIGH PRIORITY	Operator distraction, lack of competency or unavailability, control system failure, fill station plant (valve/ pump) failure	Install SIS that Interlocks filling system so filling is automatically stop if tanker High High Level reached or liquid of vapour releases are detected in environment or equipment/ sensor/comms faults are detected
Excavator driver creates loading bay	Operator doesn't create loading bay	Operator in wrong position - too far from excavator or bay truck cant get into to	Operator wont be able to create a new bay if truck in existing bay.	Truck delay because it wont have bay to come into	If bay created before kicking truck out then truck in current bay moves to new bay	Productions delays - low priority if it doesn't happen often. Worst case scenario is that create bay that truck can not safely enter (e.g. drops over edge) - asset damage/loss Or truck collides with digger	Operator distractions, errors in the virtual world, error in use of interface (more likely). Digger moves after bay is created and before truck enters - system considers where digger housing is not where stick and bucket are	Evaluation of interface usability which may lead to recommendations to improve design, inbuilt exclusions zones that doesn't allow bay too close which takes into account bench/face design. Interlock on dig unit to prevent it being in bay while bucket etc in bay. Validate and confirmation process that virtual world matches physical world

Control action	Control Action NOT GIVEN	INCORRECT Control Action IS GIVEN	Control Action GIVEN AT WRONG TIME - TOO SOON/EARLY	Control Action GIVEN AT WRONG TIME - TOO LATE	Control Action GIVEN IN WRONG ORDER or FOR WRONG DURATION	Potential Consequence(s) and Significance (High priority - must address, Med priority - should address, Low priority - monitor for change, Negligable - No further action required)	Possible causes of unsafe control action	Assessment and recommendation for improving design (ISD) or controls or control systems (DiD)
			If create bay too early truck in bay will move to new bay					
			If open before dozer finishes cleaning then truck permission would not allow it to enter					
Driver pauses or suspend truck prior approaching (on foot or going around in vehicle)	Operator doesn't give command to pause or suspend truck - press button but nothing happened	Operator picks else something on screen or unpaused instead of pauses or picks wrong truck	Truck stops too early could be stopped too close to other vehicles or intersections	Truck collides with other machines, or berm/ windrows	If faulted truck you can approach without pausing/suspending it - which could be done after talking to control (using pos comms) and checking mode lights	Assuming truck is safe when it is not. So could be in line-of-fire and get run over / collision: High priority - must address	Hit wrong button, misunderstanding re mode lights, and/or after talking to control.	

Appendix C: Automated Underground Longwall Mining Case Study

Scope for automated longwall mining

The scope used for the automated surface haulage

The scope of the system under review is shown diagrammatically in Figure C1 and is described in more detail in the scope table shown in Table C1)

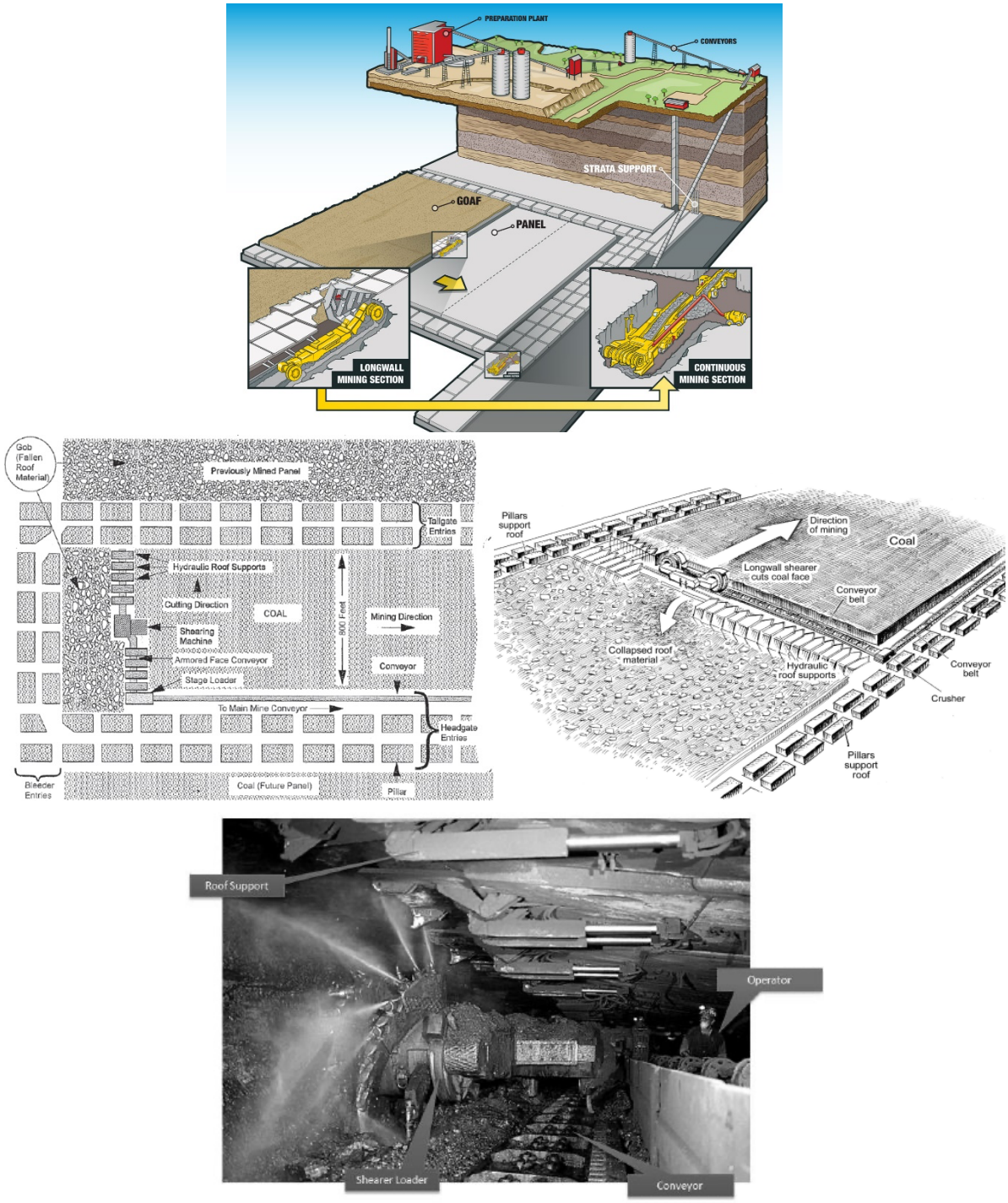


Figure C1: Overviews of underground workings and illustrations of longwall operations
(sourced from https://dougillustration.com.au/mastermyne-plant-cross-section-schematic/ https://www.nap.edu/read/25111/chapter/14#131 https://www.sec.gov/Archives/edgar/data/1037676/000095015209001922/c48697e10vk.htm and Nalbantov, et al. (2010). Image Mining for Intelligent Autonomous Coal Mining.. 17-23).

Table C1: Automated Longwall Risk Assessment Scope

Attribute of scope	Included	Excluded
P: People involved in risk management or potential impacted if risks are not managed	Employees, contractors, OEM personnel and visitors accessing areas where automated longwall and related equipment operate. Roles include: - Controllers responsible for automated operations - People who maintain/troubleshoot the automated equipment - Other personnel that enter into underground mine (e.g. supervisors, geotechnical, mining specialists etc) - IT & communications people	People not in underground mine and not involved in automated longwall operations
L: Locations or areas where the risk exist or that could be impacted if the risk event materialised	Underground areas where automated longwall mining is occurring. Location of controlling operations that are overseeing the automated longwall operations - surface or underground	Surface operations not associated with controlling automated longwall operations
E: Equipment and plant (e.g. tools, vehicles, fixed processing plant, infrastructure etc)	Automated longwall operations which includes shearer, face conveyor, shields and associated equipment, BSL & Boot end, communications infrastructure, monorail. Computer systems and software that act as part of control system for longwall	All other plant and equipment not associated with automated longwall operations e.g. main conveyor and continuous mining equipment
A: Activities (e.g. operations, maintenance, startups etc)	Longwall cutting and coal removal operations (run of face, gate end conditions, roof support movement, BSL movement, main gate push). Routine inspection while operating) Longwall maintenance operations (mechanical and electrical). Change hoses on the fly.	Activities associated with moving Longwall equipment from one panel to next Drill and blast activities. Goaf drainage activities
T: Timeframe (e.g. time based exposure info, timezone info and how far into the future)	Continuous operation – 24 hours per day, 7 days a week, all seasons of the year in Australian climatic conditions. Consideration should include shift and break changeover processes.	Adverse climate conditions – wet weather, lightning, etc.
S: Known risk scenarios that need to considered	Scenarios need to consider potentially fatality or severe injury resulting from unsafe human-automation interaction caused by: - malfunction of automated longwall equipment requiring beyond design/inadvertent/novel human interaction - malfunction/ overriding/ hacking of safety/comms systems, - non-detection of human in longwall area	Equipment fire or equipment initiated coal fire. Methane and/or dust explosion scenarios

The high risk human-system interaction activities identified during the scope are as follows:

- **Interaction with automated shearer, face conveyor and/or shield systems during production**
    - shearer operator standing on floor between roof support and pan line injured by interaction with roof support during automated longwall shield advance – eg. Crush injury from BSL _____
    - Loss of manual operation skill
- **Routine maintenance and calibration of longwall equipment and associated automated control systems:**
    - Uncertainty regarding whether longwall is in automated mode – especially during production-based maintenance. Eg., Tradesman completing maintenance leading to interaction with supports and/or shearer
    - Inadvertent operation on start-up
    - Unanticipated movement of equipment during maintenance

- **Human responding/not responding to control system guidance, safety alerts and exceptions**
    - Operators remote controlling from the field
    - Control room controllers overriding control system or misinterpreting/incorrectly handling exceptions
    - Automation system introduces catastrophic failure -
    - Loss of situation awareness through loss of access to direct interaction with longwall (eg., sound, smell, peripheral vision)
    - Misunderstanding/misinterpretation of the information provided by remote interfaces, or lack of information
    - Control room operator fatigue/distraction leads to inattention to interfaces – miss something that needs reaction
    - Change management – unintended consequences of changes – some people unaware of consequences of changes. Eg., change to cope with adverse conditions, not communicated

A decomposition of these activities was not performed. No additional assumptions or caveats were noted during the scoping exercise.

HAZID results for automated longwall mining.

The first risk assessment technique undertaken for this case study was the HAZID analysis. The results of this analysis are tabulated in Table C2 which shows the relevant information from the full HAZID spreadsheet. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table C2: HAZID analysis for Automated Longwall Mining

Description of Hazard	Unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis: Estimate of Likelihood	Risk analysis: Overall Risk Rank
Mechanical shield advancing	Personnel to shield interaction during automatic shield advancing	Breach of no-go zone = someone standing where they shouldn't be	Single fatality or lost time injury due to person being crushed b/n equipment	**4**			Major	Likely	**High Risk**
		System failure - personnel proximity detection system not working/calibrated							
		Lack of training							
	Personnel to shield interaction during manual advancing it from upstairs	Someone advances wrong shield							
		Person doesn't know operator is there							
BSL push	BSL pushed with person in unwanted area	Breach of no-go zone = someone standing where they shouldn't be	Single/multiple? fatality or lost time injury due to person being crushed b/n equipment						
		System failure - personnel proximity detection system not working/calibrated							
		System failure - cause push at wrong time							
		Lack of training							
		Person executing push remotely from surface at wrong time							
Equipment interaction	Shearer to PRS collision/ interaction	System failure	LTI - potential of being struck by something e.g. picks						
		Remotely controlled equipment causing collision							
Distraction of remote operator	Remote operator is not monitoring people and equipment underground	Surface operator distracted by phones/ visitors/ other activities (e.g on computer)	Personnel being crushed, could also be outburst or frictional ignition from not monitoring which is potential multiple fatalities						
	Remote operator not available to start/stop equipment when needed								
	Remote operator unavailabe for pos comms processes								

Analysis result is only an example, done to demonstrate how this part of spreadsheet works. Risk analysis should be done when the specific context is known

Description of Hazard	Unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis	
								Estimate of Likelihood	Overall Risk Rank
Frictional ignition	Shearer to shield interaction	System failure, equipment moved from remote position	Gas ignition = potential multiple fatalities/injuries						
	Malfunction of BSL chain, AFC chain, shearer cutting, drives	Less visual inspections done by people because less persons in vicinty of equipment and cameras have limitations (don't provide vibration, sound etc that is relied on by personnel)	Gas ignition = potential multiple fatalities/injuries						
Hydraulic	Not identifying blown hose, leaking valving etc, high pressure release event	Less visual inspections done by people because less persons in vicinty of equipment and cameras have limitations (don't provide vibration, sound etc that is relied on by personnel)	Loss of containment of hydraulic oil = might be LTI if person got hit. Probably more of a business loss.						
Energised plant	Control room activation of equipment during maintenance day	Unprotected access to system - both access to physical area and to computer system, lack of training or procedures	Personnel interaction with equipment causing crush injury						
Energised plant	Adhoc people come onto face without proximity detectors (e.g. to geomap the face)	Unprotected access to face, lack of training or procedures							
Combustible coal, hydraulics etc	Smoke on face not detected	less visual inspections done by people because less persons in vicinty of equipment and cameras have limitations	Equipment damage until it got worse enough for sensors to pick up						
Geotechnical	Loss of strata control	less visual inspections done by people because less persons in vicinty of equipment and cameras have limitations	Equipment damage due to face fall in isolated area						

FMECA results for automated longwall mining

The second risk assessment technique undertaken for the automated longwall mining case study was the FMECA analysis. The results of this analysis are tabulated in Table C3. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table C3: FMECA analysis for automated longwall mining

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
Roof supports	To support roof, advance and push AFC	Doesn't hold roof	Defective mechanical, electrical componentry	Poor strata leading to coal face slabbing or rocks falling from roof injuring people (same for auto vs manned)	5					
		Doesn't push AFC	Communication loss. Miss communication about right truck. Education/ training	Shearer to shield interaction resulting in personnel injury from material flying off under load, frictional ignition event (same for auto vs manned)						
Remote operator	PRS automatics/ operation	Network/systems comms failure	Engineering/ hardware/ maintenance failure	Operations halted because no/ wrong comms. Have to go back to manual, putting people back on face in line of dust, equipment etc						
		Personnel understanding failure	Insufficient training, distraction, lack of procedures, skill level, insufficient/ incorrect/ incomplete info from sensors, misheard/ misinterpreted info from personnel	Inadvertant operation of wrong part of equipment or wrong sequence used may resulting in harm to persons, equipment damage and/or production delay						
		Inadequately commissioned system	Lack of knowledge due to know historical data/ experience plus insufficient training/ procedures, distraction, lack of skills	Incorrect setup/ configuration of gear could lead to equipment operating outside intended paramaeters, people not understand how/when it will move resulting in LTI						
	Shearer automatics/ operation	Network/systems comms failure	Engineering/ hardware/ maintenance failure	Operations halted because no/ wrong comms. Have to go back to manual, putting people back on face in line of dust, equipment etc						
		Personnel understanding failure	Insufficient training, distraction, lack of procedures, skill level, insufficient/ incorrect/	Inadvertant operation of wrong part of equipment or wrong sequence used may resulting in						

Did not complete this section as it was not part of the workshop. Risk analysis should be done when the specific context is known

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
			incomplete info from sensors, misheard/ misinterpreted info from personnel	harm to persons, equipment damage and/or production delay						
		Inadequately commissioned system	Lack of knowledge due to know historical data/ experience plus insufficient training/ procedures, distraction, lack of skills	Incorrect setup/ configuration of gear could lead to equipment operating outside intended parameters, people not understand how/when it will move resulting in LTI						
		Shearer/ cutting induced frictional ignition event	Condition of picks unknown	Potential ignition of gas leading to multiple injuries/ fatalities						
			Shearer strikes another piece of equipment	Potential ignition of gas leading to multiple injuries/ fatalities						
	AFC automatics/ operation - transportation of coal from face to conveyor	Automated equipment malfunction	Not identifed malfunction because no one located near equipment	Minimal risk to humans as not located near equipment						
		Dilution of coal	Not identifed issue because no one can see stone coming down conveyor	Material spilling on walkways so trip hazard						
		Broken/ damage/ blocked chain	Not identified foreign object or equipment issue because no one located near equipment	Minimal risk to humans as not located near equipment but if people at maingate (eg looking at blockage, on face side of AFC), risk could be LTI/ fatality from recovery process (e.g. from face coal, released tension)						
		Frictional ignition from chain/ conveyor	Not identified foreign object or equipment issue because no one located near equipment	Potential ignition of gas leading to multiple injuries/ fatalities						
	BSL push operations	Network/systems comms failure	Engineering/ hardware/ maintenance failure	Operations halted because no/ wrong comms. Have to go back to manual, putting people back on face in line of dust, equipment etc						

Not completed in workshop due to time constraints

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
		Personnel understanding failure	Insufficient training, distraction, lack of procedures, skill level, insufficient/ incorrect/ incomplete info from sensors, misheard/ misinterpreted info from personnel	Inadvertant operation of wrong part of equipment or wrong sequence used may resulting in harm to persons, equipment damage and/or production delay						
		Inadequately commissioned system	Lack of knowledge due to know historical data/ experience plus insufficient training/ procedures, distraction, lack of skills	Incorrect setup/ configuration of gear could lead to equipment operating outside intended paramaters, people not understand how/when it will move resulting in LTI						
		Interaction with belt system	Insufficient training, distraction, lack of procedures, skill level, insufficient/ incorrect/ incomplete info from sensors, misheard/ misinterpreted info from personnel	People at outbye could be affected if tear belt resulting in recordable/ long-term injury						
Communication systems - surface to face comms	Positive comms between human to human at face and surface	Incorrect application (e.g. shearer sent in wrong direction, wrong shield moved)	Incorrect information from face or surface	Single fatality from moving shield where person standing						
	Positive comms between human and interfaces at face and surface	Incorrect application (e.g. shearer sent in wrong direction, wrong shield moved)	Incorrect information from interface	Single fatality from moving shield where person standing						
	Telecommunication system to convey information	Unclear communications	Incorrect information	Single fatality from moving shield over someone or pulling pan back						
		Loss of digital communicaitons	No information	No movement of equipment - no risk						

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
Maintenance	Software/data updating	Incorrect/ incomplete/ faulty software upgrade	Faulty software, lack of programming oversight, incorrect installation	Unexpected/ unplanned movement of equipment leading to injury/ fatality						
		Operators do not understand updates to logic changes	Lack of change management / training	Fatality from unexpected movement of equipment						
	Humans maintaining/ calibration around operating autoomous equipment	Incorrect calibration of equipment - e.g. tilt sensors on shields, anticollision systems	Lack of knowledge, insufficient training	Interaction of equipment with the potential to injury people. Potential for frictional ignition leading to multiple fatalities						
		Incorrect maintenance	Lack of knowledge, insufficient training	If not maintained correctly, remote operation will not work						
		Incorrect understand of process - what equipment is operating and its operational mode	Lack of knowledge, insufficient training, lack of indication (e.g. lights on entry, machine, face)							

SAfER results for automated longwall mining

The third risk assessment technique undertaken for the automated longwall mining case study was the SAfER analysis. The results of the situation assess part of the SAfER analysis are tabulated in Table C4. The results from the strategies analysis part of SAfER is shown in Table C5.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

Table C4: Situation assessment part of SAfER analysis for the automated longwall

Situation Assessment Indicators	List the indicators that need to be monitored to check for safe/unsafe operation?	What design improvements could make these indicates easy to perceive, comprehend and project into the future?
Plant/process factors	'What operating mode Sensor healthy. All systems operating as required. Vision were required. External monitoring available. Status of commissioning, daily and weekly inspections Interface - colours/indicators, critical alarms - available both surface and underground Equipment report - on how caving report and shield/leg pressures etc	'Lighting system to show operational mode e.g. maintenance, remote controlled operations Lighting/alert system to tell person underground when movement about to happen Sensor suite to show status system - to tell what environment is underground.
People factors	'Where is the authority to operate. People understand their roles and position Individuals' competencies Personnel position monitoring	Lighting system to show when someone enters no-go zone - illuminates red light to highlight breach Personal proximity detection with fail safe links to no-go zone procedure and EMS if loss detected
Context factors	'Access requirements Strata reports - how cutting seem	'Tiered access provided to those with requisite competencies who require access with alerts when unauthorised access to computer systems. Measurement of strata status

Table C5: Strategies analysis part of SAfER (blue is normal operations, purple is abnormal operations)

Generic Strategy Prompts	**What plausible decision/actions related to this generic strategy could be used in the system being analysed?** (Consider examples for both normal and abnormal operations)	**What consequences might result if people adopt this strategy?**	**Should design promote, prevent or tolerate strategy?**	**What design improvements would improve response strategies during normal, abnormal and unexpected situations?**
Avoidance = Not done, defer, or forget to do	Control operator - Not stop or start operation because distracted	Safety or production incident could	Prevent	Restrict access to room. Ergonomically design room. Prevent use of personal electronic devices. Presence/vigilance detection interlock with safety shutdown
Intuitive = automatic response, done without explicitly or deliberately using thought processes				
Arbitrary-choice = guessed, scrambled haphazard or panicked response	Control operator "guesses" which shield to activate	Person under shield who is in harms way	Prevent	Automation to remove guessing, along with training and competency
Imitation strategies = copy how others do it or copy what has worked in the past	Operator copies floor correction	Potential loss of horizon	Prevent	Training competencies and systems. Use limits to constrain amount of correction allowed.
Cue-based strategies = select Chosen Option using the Observed Info/Cues and Predict Consequences results				
Compliance-based strategies = following procedures as they are written/practiced				
Analytical Reasoning strategies = using analytical thinking to reason out the best way to perform task				

Incomplete due to workshop time constraints

STPA results for automated longwall mining

The fourth risk assessment technique undertaken was the STPA analysis. The results of the control diagram are shown in Figure C2. The results from the risk identification part of STPA analysis is shown in Table C6.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

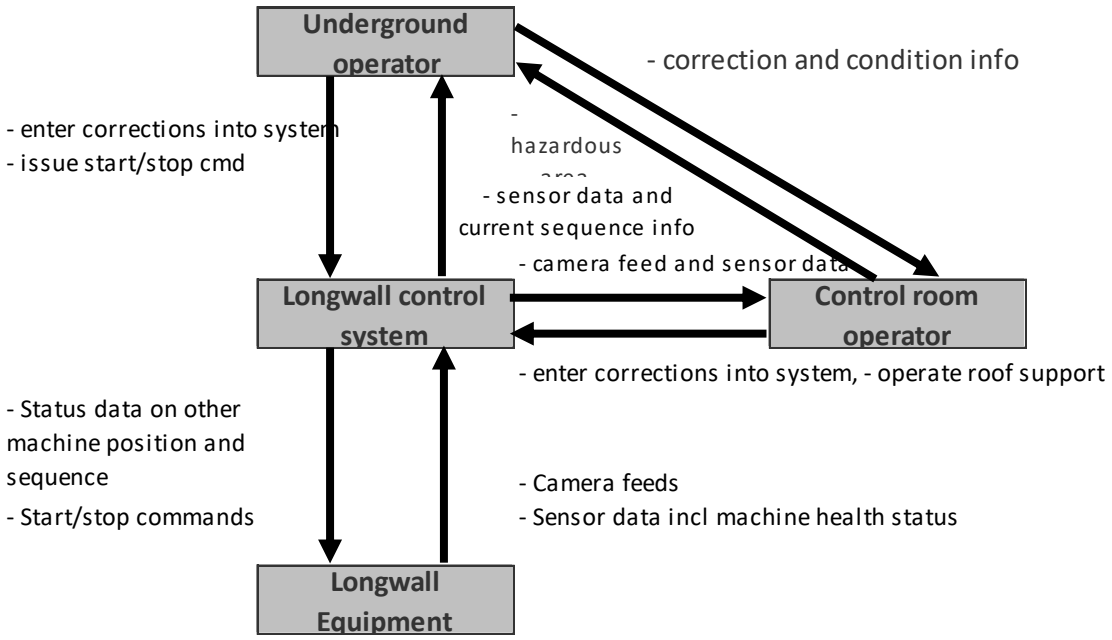


Figure C2: Human system interaction control diagram

Table C6: STPA analysis for autonomous haulage

Control action	Control Action NOT GIVEN	INCORRECT Control Action IS GIVEN	Control Action GIVEN AT WRONG TIME - TOO SOON/EARLY	Control Action GIVEN AT WRONG TIME - TOO LATE	Control Action GIVEN IN WRONG ORDER or FOR WRONG DURATION	Potential Consequence(s) and Significance (High priority - must address, Med priority - should address, Low priority - monitor for change, Negligable - No further action required)	Possible causes of unsafe control action	Assessment and recommendation for improving design (ISD) or controls or control systems (DiD)
Operate roof support	Longwall production stops	Wrong roof support moved	Support could collide with shearer	Support could collide with shearer	Wrong roof support moved	Wrong chock moved could lead to a fatality. High priority that must address	Cause of moving wrong roof support: Lack of training, competence, overriding of automation or issues with automation interlocks	
		Operate wrong function - e.g. lower instead of raising	Break pins and hoses on the support	Break pins and hoses on the support	Equipment damage if lowered too far			
Operator stop system when coal boiling over AFC	Spill tray fills with debris coal	Same as control action not given	AFC stopped before boil over (will stop production = loss of production)	Lot more material in spill tray and walkway (extends production delay)	In stop/start, stop/start scenario - could cause delays in production	Production delay, damage to shearer cable	Loss of situation awareness (e.g. out of view of camera), people thinking boil over wont happen or will clear, environmental e.g. slabbing of coal that causes blockages	
	Walkway fills up with debris coal				AFC stopped but not shearer cutting - cause worst spill without interlock.	Production loss and restricted access due to blocked walkway		

Appendix D: Remote operated coal preparation plant

Scope for remotely operated coal preparation plant

The scope used for the remotely operated coal preparation plant case study is shown diagrammatically in Figure D1 and is described in more detail in the scope table shown in Table D1.

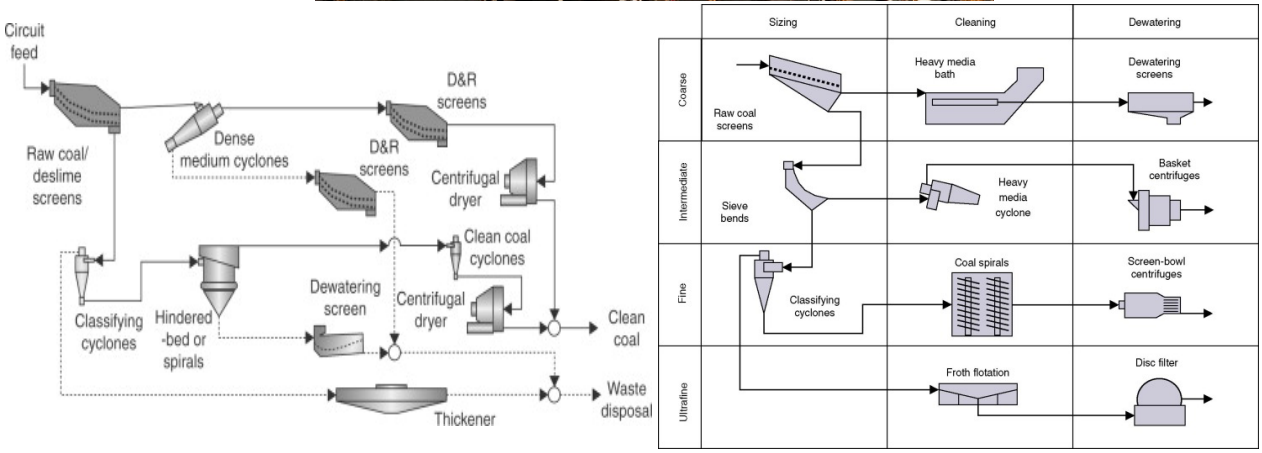


Figure D1: Overviews of coal processing plant operations

(sourced from https://www.hitachi.com/rev/archive/2018/r2018_01/pdf/P087-092_R1a07.pdf and https://home.komatsu/en/company/tech-innovation/solution/) https://www.ausenco.com/en/carborough-downs-chpp ; http://iminco.net/chpp-operator-maintenance-coal-mining-electrical-trade-qld-iminco/ ; 14 - Economic factors affecting coal preparation: plant design worldwide and case studies illustrating economic impact. In D. Osborne (Ed.), *The Coal Handbook: Towards Cleaner Production* (Vol. 1, pp. 445-466): Woodhead Publishing. Robert A. Meyers et al "Coal Preparation", in Encyclopedia of Physical Science and Technology (Third Edition), 2003 and Bethell, P. J. (2013).

Lastly we describe some of the top high risk human-system interactions then decompose in functional terms to ensure fully range of interaction possibilities are considered in the risk assess. The high risk activities to be explored in this study are as follows:

RISK SCENARIOS DESCRIPTIONS

The decomposition is shown in Table D1.

Table D1: Functional Decomposition of risky human-automated systems interactions

Interaction	Description of functions to consider	Comments/Issues to consider
1. Undetected malfunction leading to falling rocks, slurry etc due to: ○ Excess water – on conveyors/materials handling streams ○ Undetected blockages ○ Failure in slurring piping ○ Failure of equipment (e.g. conveyors)	6. Coal being dumped into hoppers 7. Coal being conveyed and transferred between conveyors 8. Coal being stacked onto stockpiles with stackers 9. Coal being reclaimed from stockpiles with reclaimers and/or bulldozers 10. Slurry material being pumped/piped around plant	• • •
2. Bridged/malfunction/ overriding of control system/alarms due to ○ Operators remote acknowledge alarms without addressing ○ Control room controllers overriding control system or misinterpreting/incorrectly handling exceptions ○ Inadvertent changes to parameters/code ○ Unexpected failure of equipment	1. Controllers do not have [full] situation awareness on site so treatment of alarms is done at own discretion with/without feedback from field operators. 2. Overriding control system is typically done during testing/ commissioning and startup. These overrides could include . . . . [tbd} 3. Bridging, changing parameters or other code changes is usually done by technicians/ engineers to keep plant running/ update code/ change operations. Examples include . . . . 4. Unexpected failure or malfunction of control system componentry could can overall function of control system	• • •
3. Non detection of humans involved in troubleshooting/ cleaning/ maintenance activities:	1. Washing down equipment 2. Unblocking blockages 3. Condition monitoring equipment while plant is operating 4. Maintaining equipment while plant is operating 5. Bringing equipment back on line. 6. Operating mobile equipment (e.g. loader, dozer, bobcat) in and around remote controlled plant	• • •

Table D2: Autonomous Surface Haulage Risk Assessment Scope

Attribute of scope	Included	Excluded
P: People involved in risk management or potential impacted if risks are not managed	Employees, contractors, OEM personnel and visitors accessing processing plant areas and/or remote control operations areas. Roles include - Controllers who manage processing plant operations - People who are in charge of cleaning and maintaining plant - Other personnel entering into plant or remote control room areas (e.g. supervisors, cleaners, engineers, sampling people, lab people and authorised and unauthorised visitors etc) - IT & communications people - Training load out station personnel (e.g. local or remote)	People outside the plant and remote control operational areas.
L: Locations or areas where the risk exist or that could be impacted if the risk event materialised	Surface processing plant areas - Processing plant from ROM load station to product stockpile to train load out - Remote control room location - Location of critical communications infrastructure (e.g. radio, CCTV and control system), MCCs and control system components	Areas upstream of load station and downstream of train load out station.
E: Equipment and plant (e.g. tools, vehicles, fixed processing plant, infrastructure etc)	Processing plant equipment and control system components which includes - Plant load station (e.g. rail, ROM, etc) - Conveyors, transfer chutes for feed, product, waste etc - Processing plant sizing, washing and dewatering screens, crushers, cyclones, pumps, pipes and fittings etc. - Mobile equipment used around plant e.g. loaders/bobcats/bulldozers - Product stackers/reclaimers for loading on/off stockpiles. Train loading equipment	Tailings reject and disposal Ancillary/Potable water treatment processes? Train
A: Activities (e.g. operations, maintenance, startups etc)	Conveying, sizing and washing of coal, stacking/reclaiming and load coal onto train, in-field troubleshooting, equipment cleaning, and maintenance. Human-system interactions include: - Manual cleaning - Troubleshooting faults - Manual inspecting, condition monitoring and minor adjustment - Lab sampling - Maintenance (on equipment offline while plant is operating) - Mobile equipment tasks e.g. loading of hopper, pushing stockpiles, plant cleanup, - Shutdown and startup interactions for shutdowns	Decommissioning and commissioning of plant Movement of train through load station

T: Timeframe (e.g. time based exposure info, timezone info and how far into the future)	Continuous operation – 24 hours per day, 7 days a week, all seasons of the year in Australian climatic conditions. Consideration should include shift and break changeover processes Adverse climate conditions – wet weather, lightning, dust, fog, ice, and extreme heat/high temperatures.	
S: Known risk scenarios that need to considered	Unsafe human-automation interactions which could result in fatality or severe injury resulting from unsafe human-automation interaction caused by "caught by/struck by type events i.e.: - Non-detection of human involved in troubleshooting/ cleaning/ maintenance activities - Undetected malfunction leading to falling rocks, slurry etc - Malfunction/ overriding/ hacking of safety/comms systems, -	Equipment fire or equipment initiated coal fire. Structural failures

The potential future risk scenarios that could be considered are:

- **Undetected malfunction leading to falling rocks, slurry etc due to:**
    - Excess water – on conveyors/materials handling streams
    - Undetected blockages
    - Failure in slurring piping
    - Failure of equipment (e.g. conveyors)

- **Bridged/malfunction/ overriding of control system/alarms due to**
    - Operators remote acknowledge alarms without addressing
    - Control room controllers overriding control system or misinterpreting/incorrectly handling exceptions
    - Inadvertent changes to parameters/code
    - Unexpected failure of equipment

- **Non-detection of humans involved in troubleshooting/ cleaning/ maintenance activities:**

The high risk activities for decomposition are as follows and the decomposition is shown in Table D3.

TableD3: Functional Decomposition of risky AHS interactions

Interaction	Description of functions to consider	Comments/Issues to consider
1. Undetected malfunction leading to falling rocks, slurry etc due to: ○ Excess water – on conveyors/materials handling streams ○ Undetected blockages ○ Failure in slurring piping ○ Failure of equipment (e.g. conveyors)	• Coal being dumped into hoppers • Coal being conveyed and transferred between conveyors • Coal being stacked onto stockpiles with stackers • Coal being reclaimed from stockpiles with reclaimers and/or bulldozers • Slurry material being pumped/piped around plant	• • •
2. Bridged/malfunction/ overriding of control system/alarms due to ○ Operators remote acknowledge alarms without addressing ○ Control room controllers overriding control system or misinterpreting/incorrectly handling exceptions ○ Inadvertent changes to parameters/code ○ Unexpected failure of equipment	• Controllers do not have [full] situation awareness on site so treatment of alarms is done at own discretion with/without feedback from field operators. • Overriding control system is typically done during testing/ commissioning and startup. These overrides could include . . . . [tbd} • Bridging, changing parameters or other code changes is usually done by technicians/ engineers to keep plant running/ update code/ change operations. Examples include . . . . • Unexpected failure or malfunction of control system componentry could can overall function of control system	• • •
3. Non detection of humans involved in troubleshooting/ cleaning/ maintenance activities:	7. Washing down equipment 8. Unblocking blockages 9. Condition monitoring equipment while plant is operating 10. Maintaining equipment while plant is operating 11. Bringing equipment back on line. 12. Operating mobile equipment (e.g. loader, dozer, bobcat) in and around remote controlled plant	• • •

No additional assumptions or caveats were noted during the scoping exercise.

HAZID results for remotely operated coal preparation plant

The first risk assessment technique undertaken was the HAZID analysis. The results of this analysis are tabulated in Table D4 which shows the relevant information from the full HAZID spreadsheet. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table D4: HAZID analysis for Autonomous Surface Haulage

Description of Hazard	Unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis	
								Estimate of Likelihood	Overall Risk Rank
Energised (mechanical / electrical) plant	Equipment started without request	Incorrect coding, field operator starts without CRO permission, CRO starts without field notification	People caught in rotating equipment, incorrect processing, equipment damage. Most likely occurrence would be single fatality	4			Major	Likely	High Risk
	Incorrect equipment started	Miscommunication (not clear radios, delays in comms between site and control system), operation error							
	Equipment failed catastrophically	Poor maintenance, incorrect installation of equipment, equipment overloaded/blocked	Serious injury to people in proximity of equipment						
Differences between coal mine and whs acts, and different regs between state	Unknowing giving access of people in plant areas that are not safe	Conflicting instructions between two different people. Not including / not notifying control personnel in risk assessment processes	Potential for dropped objects, person crushed by something, interaction between people and vehicles						
	Multiple people giving instructions to maintenance making it hazardous for people to enter or operate	Same as above plus poor communication between workgroups	As above						
	Deisolation of equipment without informing all work parties and commissioning interactions associated with making sure equipment is ok to hand back to operations	Same as above plus using non-standard/non-uniform practices	Falling objects, inundations, crushing, electrical shock, entanglement in moving parts						
Inaction between coal mining and CPP (access, dumping on ROM etc)	Falling rock from ROM when person underneath	Dumping when not requested, misaligned dumping, failure of comms associated with person accessing under/on top of ROM	Rocks falling on people, damage to ROM bin structure, truck fall into bin						
Communication failures	Loss of comms between equipment (e.g. stacker and reclaimer working on same stockpile)	Manual controlling and mismatched understanding of what system will/wont do in local control, remote comms issues. Incomplete/incorrect handover during crib and shift changes	Equipment damage, personal injuries is cannot tell piece of equipment to stop						

Description of Hazard	Unwanted event scenarios	Causes	Consequences	People	Assets	Environment	Max Impact	Risk analysis	
								Estimate of Likelihood	Overall Risk Rank
Situation awareness	Loss of awareness of situation in plant (what is happening/planned)	Incomplete/incorrect handover during crib and shift changes. Supervisors not notifying control of testing and other activities happening	Equipment damage with possibility of fatality						
Energised (mechanical / electrical) plant	Equipment - vehicle interactions/collisions	Parked in wrong spot, parked vehicle in area not safe when equipment in manual. Person controlling equipment not aware of vehicles in area. Did not believe isolation of equipment was required	Equipment damage, personal injuries with possibility of fatality						
Energised (mechanical / electrical) plant	Isolation failure - piece of equipment is left unisolated	Poor procedures, poor understanding of systems involved, lack of awareness of every piece of gear that needs to be isolated	Potential fatality/injury and damage to equipment						
Gravity. Engulfment of coal	Incorrectly operation of plant (e.g. opening up coal valve)	Instruction not followed. Failure to detect and action alarms. Miscommunication between site and control. Insufficient training so people understand of potential issues	Dozer on top drawn into valve/buried with potential health issue/injury/fatality. Potential to cause damage to belt underneath As above						
	Third party interactions associated with controlling equipment (e.g. control centre, third party and site personnel)	Poorly trained, insufficient controls to prevent unauthorised access							
	Unsafe interaction with two separate autonomous systems i.e. the AHA on ROM (e.g. Truck can dump when it feels like (doesn't require plant permission)	Using wrong procedure or doing procedure incorrectly, lack of awareness of plant procedures e.g for accessing under ROM. Don't include sufficient plant people in risk assessment	People may be working under ROM when truck dumps - and could be struck by falling ore						
	Inadequate emergency response	Insufficient resources available to respond. More people working alone - if accident happens may not be able to call emergency response	Fatalities						

FMECA results for remotely operated coal preparation plant

The second risk assessment technique undertaken was the FMECA analysis. The results of this analysis are tabulated in Table D5. **It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.**

Table D5: FMECA analysis for remotely operated coal preparation plant

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
Control room operator	Commands given by control room operator	Incorrect comands leading to something tipped when not supposed to, belt stopped in full motion, unplanned start ups and stoppages	Lack of training, lack of concentration, distraction, incorrect coding, miscommunication between two systems	Spillage, overloads, blockages, incorrect processing which could cause injuries to personnel and equipment damage.	5					
Software	Commands delivered by software coding	Incorrect command leading to failure to work/ incorrect operation of interlocks, equipment operating out of sequence	Not testing system before going live, incorrect inputs used for coding, not following procedure, unforeseen interactions between codes under certain circumstances, bypassing code	As above plus continuing to run equipment when it should be stopped						
Control room operator or maintenance personnel	Driving equipment in manual or using manual overrides	Equipment starting or continues to run when not required, operating outside of OEM specs	Driving something in manual without understanding upstream/downstream impacts, personnel not aware of other issues on plant.	As above plus engulfment from material falling out of bins with the potential of a fatality						
Control system infrastructure	Communication between equipment, between control room and equipment, between control room operator and people	Communication loss (e.g. stacker and reclaimer failing to communicate with each other)	Lag/delays in comms, personnel response time, damage of equipment, loss of power/internet, partial comms loss (e.g. just lose radios), ransomware attack, multi users giving conflicting instructions	Depends on part of plant affected but could result in the inability to control equipment which might result in equipment damage (e.g. due to collisions, continuing to run equipment when it should be stopped), and human injuries/fatalities (e.g.due to falling ore, entanglement, struck by object)						
Control system infrastructure	Communication between control system components	Communication loss between multiple autonomous subsystems	Corrupted blocks, router issues, mismatch between systems and codes, new emerging systems							

Did not complete this section as it was not part of the workshop. Risk analysis should be done when the specific context is known

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
ROM	Trucks only tip when safe at ROM	Trucks tip when person on/ under ROM, truck tips when ROM not clean, truck tips when ROM full, trucks tipping into ROM bin when maintenance occurring, incorrect blends put in ROM, ROM not isolated when people in area	Changes in system/ procedures that people not familiar with, miscommunication between AHA and plant systems, AHA controlling when they dump without understanding implications on plant, lack of training, inability to isolate ROM due to unable/not being locked out, plant people to do have ability to apply stop for AHA activity on/near ROM	Potential for rocks falling on people leading to fatalities/injuries, damage to equipment, production impact due to incorrect blends						
Plant	Manual intervention (e.g. to sample)	Inadequate barriers/ protections in automation areas to protect people	Plant design not designed for people entering. People do not have ability to apply a stop to equipment in area they are entering	Potential for entanglement						
TLO	Dozer operators pushing coal into coal valves	Brake failure on dozer, voids in coal, dozer unable to stop loadout, miscommunication leading to dozer above active valve	Mechanical failure e.g. due to poor maintenance/ overuse, not following procedure, communication failure between control room and dozer	Burying dozer leading to engulfment and health issues and injuries for driver						
Communication system (level sensors)	Control bin levels	Bin level sensor failure, miscommunication between two systems	Poor maintenance/ calibration, buildup of dust on sensors	Incorrect batching (both high and low) resulting in overflow of rail car and bunker. Could derail train due to incorrect weights in cars						
Operator	Checking that wagons are filled and that control system is running as it should	Failure to respond to exception alarms, failure to detect/ respond to issues with control systems	Overloading operator - Dealing with other critical plant issues so unable to attend to TLO, lack of screens, unable to do trending to predict issues, information							

Component Name	Component Function	Failure Mode(s)	Cause(s) of Failure	Effects of Failure	People	Assets	Environment	Max Impact	Risk analysis	
									Est Likelihood	Overall Risk Rank
			overload from many screens, cameras, radio/phone comms, poor interface/system design i.e. issues with alarm flood, and alarm mgt - how do you ensure alarms are detected, actioned and not cleared before actioned							
	Operators actioning of alarms	Failure to respond to exception alarms, failure to detect/ respond to issues with control systems	Overloading operator - Dealing with other critical plant issues so unable to attend to alarms, lack of screens, unable to do trending to predict issues, information overload from many screens, cameras, radio/phone comms, poor interface/system design i.e. issues with alarm flood, and alarm mgt - how do you ensure alarms are detected, actioned and not cleared before actioned. People still under training/ learning the system, operator not familar with equipment and making incorrect conclusions or going to wrong equipment	Extended downtime, incorrect dumping at ROM, unplanned shutdown/ startup of equipment leading to equipment damage, operator mental fatigue/ stress (resulting in lower performance)						

SAfER results for remotely operated coal preparation plant

The third risk assessment technique undertaken was the SAfER analysis. The results of the situation assess part of the SAfER analysis are tabulated in Table D6. The results from the strategies analysis part of SAfER is shown in Table D7.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

Table D6: Situation assessment part of SAfER analysis

Situation Assessment Indicators	List the indicators that need to be monitored to check for safe/unsafe operation?	What design improvements could make these indicates easy to perceive, comprehend and project into the future?
Plant/process factors	Presence of system alarms (notification, followed by safety shut) for compressor air receiver pressure, wagon weight monitoring system, fire alarms, gas alarms. Confirmation of isolation before person enters area. What bypass/manual functions in use - for related equipment in system Loss of containment/ overflowing of coal that could lead to being struck by falling coal or engulfment. Reclaim belt running and ore is flowing, Presence of voids	Compressor air pressure and trends and where it sits with respect to set points Exclusion zones under belts/overflow detection on belts/chutes' Interlock/personal locks to prevent valve opening when dozer near/above Stockpile valve traffic lights visible to dozer driver showing what system is doing AHA stop capabilities around ROM so system will stop if person present Downstream areas receiving materials starts up in right order and is running before loading the upstream equipment
People factors	Person's allowed to rationalise alarms and what the alarm rationalisation is. Who has physical/virtual access to equipment/area and what authorities, activities or changes in activities are occuring.	Restricting access to users and notification log of people accessing system and tasks performed Standardise alarm rationalisation process
Context factors		

Table D7: Strategies analysis part of SAfER (blue is normal operations, purple is abnormal operations)

Generic Strategy Prompts	**What plausible decision/actions related to this generic strategy could be used in the system being analysed?** (Consider examples for both normal and abnormal operations)	**What consequences might result if people adopt this strategy?**	**Should design promote, prevent or tolerate strategy?**	**What design improvements would improve response strategies during normal, abnormal and unexpected situations?**
Avoidance = Not done, defer, or forget to do	Not responding to alarm e.g. happened ten times and hasn't been an issue so just accept/acknowledge it	Miss a really problem that are actually a problem	Tolerate	Alarm log analysis per equipment and raise work order for repeat alarms. Standard process for alarm rationalisation to remove excessive alarms Dashboard showing active alarms.
	Close out a work order because it has been deferred but not new work order created to order new parts	Ignore alarms and continue to ignored it because false alarm but this continues after repair made and might miss real issue	Tolerate	SAP should have a tick box requiring a statement as to whether the work order has been completed, a new work order opened or the work order has just been closed with nothing done.
Intuitive = automatic response, done without explicitly or deliberately using thought processes	Diagnosing problem prior to it tripping/causing upset is what experienced guys do, new guys wait for alarms to be represent then respond Experience people look for causes of alarms	Experience people response is faster and leads to lower downtimes Biggest issue is people not understanding cascade loop and autocontrol does	Promote	Written cascade loops explanation provided in training. Added dotted lines on mimic pages/front page interfaces Need to provide numbers not just status lights
Arbitrary-choice = guessed, scrambled haphazard or panicked response	Operator goes to wrong piece of equipment to confirm operational status often because new person (who doesn't want to sound dumb) on site or miscommunication and equipment with similar number or refresher training/area familiarisation is not done.	Extended downtime, incorrectly isolate or isolate wrong piece of equipment and work on something that is live.	Prevent	Want to remove arbitrary choice. Refresher area training, clear labelling equipment with unit number and name, load up into computer system what is expected to be isolated/not isolated so control room can check. Colour coding twin systems so they are clearly differentiated.
Imitation strategies = copy how others do it or copy what has worked in the past				
Cue-based strategies = select Chosen Option				

Incomplete due to workshop time constraints

using the Observed Info/Cues and Predict Consequences results				
Compliance-based strategies = following procedures as they are written/practiced				
Analytical Reasoning strategies = using analytical thinking to reason out the best way to perform task				

STPA results for autonomous surface haulage

The fourth risk assessment technique undertaken was the STPA analysis. The results of the control diagram are shown in Figure D2. The results from the risk identification part of STPA analysis is shown in Table D8.

It is important to note that the focus of the exercise was to identify and document hazardous human-system interactions. It was not to rigorously assess the risk and not work was done to identify risk controls.

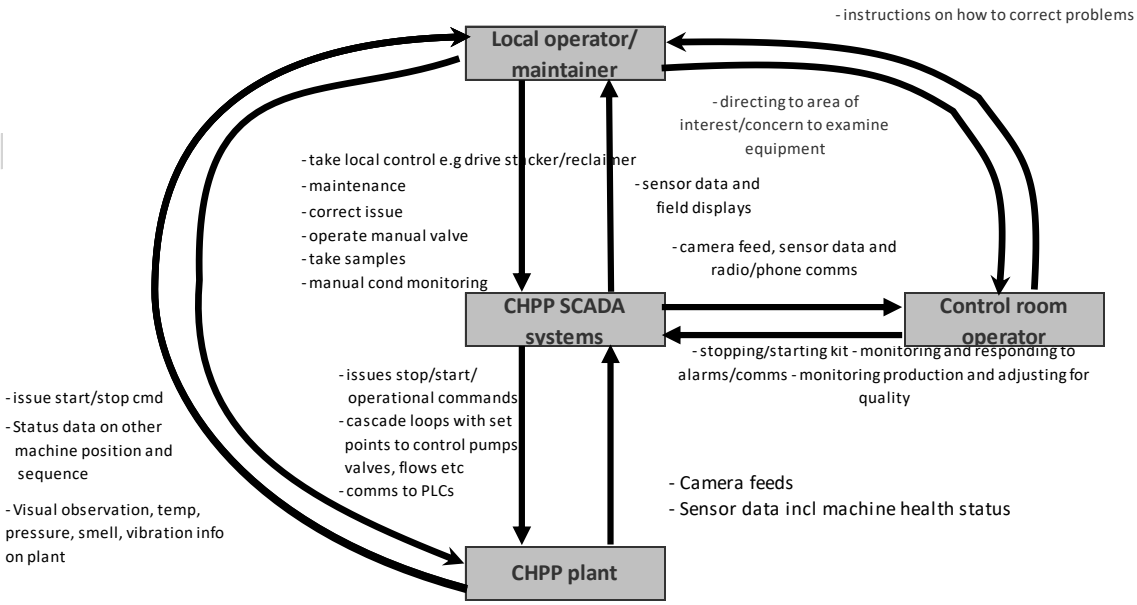


Figure D2: Human system interaction control diagram

Table D8: STPA analysis for autonomous haulage

Control action	Control Action NOT GIVEN	INCORRECT Control Action IS GIVEN	Control Action GIVEN AT WRONG TIME - TOO SOON/EARLY	Control Action GIVEN AT WRONG TIME - TOO LATE	Control Action GIVEN IN WRONG ORDER or FOR WRONG DURATION	Potential Consequence(s) and Significance (High priority - must address, Med priority - should address, Low priority - monitor for change, Negligable - No further action required)	Possible causes of unsafe control action	Assessment and recommendation for improving design (ISD) or controls or control systems (DiD)
Taking local control stacker/ reclaimer to rectify issue	Issue remains unaddressed	Stacker not put in local and still controlled by control room Reclaimer run incorrectly (e.g. bucket run in reverse)	Crash plant by taking system out of sequence	Delay is addressing issue	Crash plant by taking system out of sequence or delay addressing issue	Production losses, equipment damage (e.g. cable reelers not reeling), collision into objects	Lack of training, familarity with task, incorrect coding (e.g. when put something in local you drop out a lot of protections), distracted operator, rushing to do	**Taking local control stacker/ reclaimer to rectify issue**
Monitoring and responding to camera feed e.g. for loading wagon/ship	Cannot check whether alarm is valid. Miss rooster tails (coal too high to pass under bridges/ powerlines) on wagon	Check wrong camera, not checking camera because checking other parts of plant/ interface	Check before wagon full. So not checking status when full	Miss checking some wagons - not observed or seen causing potential failures on third party line	Same as previous - could miss multiple wagons	Spillages, derailment of train, outages of train network, extended loading times while back trains up if it get detected, damaging cables between wagons	Lack of training, distractions from other processes that you are in control of, information overload.	**Monitoring and responding to camera feed e.g. for loading wagon/ship**
Isolation of ROM for access under bin	Trucks keep dumping resulting falling materials.	Eg someone stops ROM not bin. Truck could still dump	Down longer than needs to be be	Trucks keep dumping because isolation not performed	Equipment could be damaged if not done in timely manner e.g. blockages cause damage	Spillage, equipment damage, falling objects injuring/killing people	Misinterpretaion of what is ROM due to multiple terminology	**Isolation of ROM for access under bin**