A risk-based approach to the acquisition of electronic safety equipment for mines

GPR van der Merwe

12597716

Thesis submitted for the degree *Doctor Philosophiae* in Development and Management Engineering at the Potchefstroom Campus of the North-West University

Promoter Prof JEW Holm

November 2014

Acknowledgements

I would like to thank the following people for their contributions throughout the project and for making this project possible.

Firstly, I would like to thank my promoter, Professor Johann Holm, for the exceptional way in which he guided this project through motivation, advice, and support. Also for his patience, reviews and exceptional insight towards the research topic, and for sharing his years' worth of experience with me.

THRIP, for partly funding the research study.

My family and friends for their inputs, support and motivation.

To my wife, Hanli, thank you for your love, understanding and support through these times. I would like to dedicate this thesis to you and our sons, Hanro and Marnus.

Also to the Lord, for giving me strength to endure through tough times, and for blessing the success of this project

Abstract

This research is focused on the acquisition of electronic safety equipment for mines and was conducted within the design science research (DSR) framework. Design science research ensured a directed research process was followed.

The existing acquisition process and risk management methods used in the South African mining environment were analysed by means of observations, a case study, technical documentation and literature. It was evident from this analysis that a discontinuity existed between the acquisition and operations phases in terms of the management of safety risk in the acquisition of electronic safety equipment when viewed from a full life cycle perspective. This discontinuity could be addressed by defining a risk perspective on acquisition, as such a perspective would draw together engineering and mining operations in terms of safety and productivity.

Research topics in this literature study include risk definition and terminologies, risk management frameworks, risk analysis methodologies and characterization, existing risk assessment tools and techniques, human error and operational modelling, and systems engineering. A literature study showed that similar challenges existed in other disciplines, with proposed solutions, but the discontinuity between the acquisition and operational phases had not been addressed. A specific approach of this research was to derive individualised research challenges aligned with the main research challenge, and then to translate each research challenge into one or more research solutions.

The discontinuity between the acquisition and operational phases (engineering and mining) is addressed by an activity-based risk (ABR) acquisition process. The activity-based risk method forms part of preliminary design of a systems engineering life cycle, as this phase is of critical importance to the ABR acquisition process. The focus of the ABR acquisition process is to find the functional definition and configuration of safety equipment that addresses both safety and productivity when taking into account human performance variability. In doing so, a balance between productivity and safety is found in a relativistic sense.

The effectiveness of the ABR process was verified in a real-world case study, where a safety system was analysed, fully developed, and evaluated in an operational environment to address safety risks associated with winch scraper operations.

Characteristics of the ABR process were demonstrated in this case study, which also showed in detail how to develop risk- and cost-reduced equipment from a risk perspective. Feedback obtained from evaluation of the resulting safety equipment in operation was found to be consistent with the ABR model simulation results, and assisted with the validation of the winch signalling system operational model.

Details of the ABR acquisition process are presented for functional analyses, simulation model construction, human performance variability modelling, risk-related performance measurement, simulation model evaluation, trade-off analyses, and physical realisation of winch signalling system artefacts. Finally, the advantages of using an ABR acquisition process are shown to underline the effectiveness of using a risk perspective for the acquisition of electronic safety equipment on South African mines.

Keywords: Activity-based risk, risk, modelling, acquisition, electronic safety equipment

Opsomming

Hierdie navorsing fokus op die verkryging van elektroniese veiligheidstoerusting vir die myn omgewing. Die navorsing is uitgevoer deur gebruik te maak van ontwerpswetenskap navorsing (“DSR”). DSR het verseker dat ‘n gestruktureerde navorsingsproses gevolg word.

Die bestaande verkrygingsproses en risikobestuur metodes wat in die Suid Afrikaanse myn omgewing gebruik word, was geanaliseer deur middel van waarnemings, ‘n gevallestudie, tegniese dokumentasie en ander bronne uit die literatuur. Hierdie analises toon dat daar ‘n diskontinuïteit bestaan tussen die verkryging en operasionele fases in terme van die bestuur van veiligheidsrisiko in die verkryging van elektroniese veiligheidstoerusting, wanneer beskou uit ‘n vol lewensiklus benadering. Hierdie diskontinuïteit kan aangespreek word deur die definisie van a risikoperspektief op verkryging aangesien so ‘n perspektief integrasie kan bevorder tussen die myn se ingenieursafdeling en myn se bedryf in terme van veiligheid en produktiwiteit.

Navorsingsonderwerpe vir die literatuurstudie sluit in die risiko definisie en terminologie, risikobestuursraamwerke, risiko analise metodologieë en karakterisering, bestaande risiko assesseringsmetodes, menslike foutontleding en operasionele modellering, asook stelselingenieurswese. Uit die literatuurstudie word aangetoon dat soortgelyke uitdagings bestaan in ander dissiplines, met voorgestelde oplossings, maar dat daardie diskontinuïteite tussen die verkrygings- en bedrfysfases nie spesifiek aangespreek word nie. ‘n Spesifieke benadering tot hierdie navorsing is om geïndividualiseerde navorsingsuitdagings te belyn met die primêre navorsingsuitdaging, waarna elke navorsingsuitdaging getransformeer kan word na ‘n navorsingsoplossing.

Die diskontinuïteit tussen die verkrygings- en bedryfsfases is geadresseer deur die aktiwiteit-gebaseerde risiko (ABR) verkrygingsproses. ‘n ABR metode vorm deel van die voorlopige ontwerpsfase van die stelselingenieurswese se lewensiklus, en hierdie fase is van kritiese belang in die effektiwiteit van die ABR proses. Die fokus van die ABR verkrygingsproses is om die funksionele definisie en konfigurasie van die veiligheidstoerusting te bepaal om sodoende beide veiligheid en produktiwiteit aan te spreek. Dit word gedoen terwyl die menslike fout en dienslewering se veranderlikheid

in ag geneem word. Sodoende kan ‘n balans bepaal word, met ‘n relativistiese benadering, tussen veiligheid en produktiwiteit.

Die effektiwiteit van die ABR proses was geverifieer in ‘n gevallestudie van toepassing op die werklikheid. In die gevallestudie is ‘n veiligheidsisteem geanaliseer (in terme van die ABR proses), volledig ontwikkel, en geëvalueer in ‘n operasionele omgewing om veiligheidsrisikos aan te spreek wat gepaard gaan met wenas skraper bedrywighede. Die karakteristieke van die ABR proses was gedemonstreer in hierdie gevallestudie en dui ook volledig aan hoe om risiko verlaagde en lae koste toerusting te ontwikkel uit ‘n risiko perspektief. Terugvoer uit die evaluering van die ontwikkelde veiligheidstoerusting in bedryf was belyn met die resultate van die ABR simulasie model.

Spesifieke inligting rakende die ABR proses word aangebied vir funksionele analises, konstruksie van ‘n simulasie model, menslike fout en dienslewering veranderlikheid modellering, risiko-gebaseerde dienslewering bepaling, simulasie model evaluering, kompromis analise, en fisiese realisering van die wenas veiligheidstelsel as ‘n artefak. Ten slotte word die voordele van die ABR verkrygingsproses aangetoon om die effektiwiteit van die gebruik van ‘n risiko benadering vir die verkryging van elektroniese veiligheidstoerusting vir die Suid Afrikaanse myn omgewing te beklemtoon.

Sleutelwoorde: Aktiwiteit-gebaseerde risiko, modellering, verkryging, elektroniese veiligheidstoerusting

Table of Contents

List of Figures

List of Tables

List of Abbreviations

DSR	Design Science Research
ABR	Activity-based risk
SIMRAC	Safety In Mines Research Advisory Council
COMSA	Chamber of Mines of South Africa
MHS	Mine Health And Safety
ILO	International Labour Organization
OH&S	Occupational Health And Safety
PPE	Personal Protective Equipment
HIRA	Hazard Identification And Risk Assessment
DMR	Department Of Minerals And Resources
SE	Systems Engineering
OHS	Occupational Health And Safety Act
MHSA	Mine Health And Safety Act
ISO	International Standards Organization
RF	Radio Frequency
SCADA	Supervisory Control and Data Acquisition
CO	Carbon-Monoxide
IEC	International Electrotechnical Commision
SANS	South African Standard

ALARP	As low as reasonably possible
HAZOP	Hazard and Operability Analysis
FMEA	Failure Modes and Effect analysis
FTA	Fault Tree Analysis
ETA	Event Tree Analysis
HumanHAZOP	Human hazard operability
HAZID	Hazard identification system
OptHAZOP	Optimal hazard and operability
PLSA	Plant level safety analysis
PHA	Process hazard analysis
RBD	Reliability block diagram
SCHAZOP	Safety culture hazard and operability
SRA	Structural reliability analysis
CEI	Chemical exposure index
FEI	Fire and explosion index
FEDI	Fire and explosion damage index
IFAL	Instantaneous fractional annual loss
RRI	Reactivity risk index
SWeHI	Safety weighted hazard index
PROFAT	Probabilistic fault tree
MOSAR	Method organised systematic analysis of risk
QRA	Quantitative risk analysis
PRA	Probabilistic risk analysis

ISGRA	International study group on risk analysis
ORA	Optimal risk assessment
IDEF	Integrated Definition
LOPA	Layers of protection analysis
WHO	World health organization
FMECA	Failure mode effect and criticality analysis
FRR	Facility risk review
STAMP	System-theoretic accident model
TAFEI	Task analysis for error identification
PHEA	Predictive human error analysis
HFMEA	Human failure modes and effects analysis
HRA	Human reliability assessment
THERP	Technique for human error rate prediction
TESEO	Empirical technique to estimate operator errors
HFIT	Human factors investigation tool
TRC	Time reliability correlation
SPAR-H	Human reliability analysis method
IDDA	Integrated dynamic decision analysis
FRAM	Functional resonance accident model
STEP	Sequentially timed events plotting
SIL	Safety Integrity Level

PRI	Process risk indicator
HFW	Human Factors Workbench
HR	Human resources
MIL-STD	Military Standard
EIA	Electronic Industries Alliance
IEEE	Institute Of Electrical and Electronic Engineers
SEMP	Systems engineering management plan
PMP	project management plan
CSIR	Council of Scientific and Industrial Research
AWS	Air-Whistle System
ESS	Electronic Signalling System
LED	Light Emitting Diode
PLF	Production Loss Factor
HEF	Hazardous Exposure Factor
PHEF	Prestart related Hazardous Exposure Factor

Chapter 1
Introduction

Operational risk has many definitions, each of which applies to a particular discipline. The management of operational risk depends on the framework, or ontology, inside which risk must be managed. The result is that different perspectives on risk resulted in different management approaches over the years.

This research started when operational risk was investigated by participating in development projects in the mining industry, particularly in deep mines in South Africa. Operational risk, and its perspectives, was also studied from literature as a wealth of literature on this research topic exists. From these different views, a generalised perspective of operational risk was extracted and used to evaluate electronic safety equipment in operation.

In any system life cycle, two major phases exist, namely acquisition and operation (including maintenance). It became obvious that significant differences existed between risk management in acquisition of a system and risk management during operation of that system. This difference was observed specifically in the mining industry, as described in more detail in sections further on in this thesis.

More specifically, the research problem was defined when a significant discontinuity was observed between engineering (responsible for acquisitions) and mining (responsible for operations) in the mining industry. Since the mining environment is highly dependent on electronic equipment for safe operations, an opportunity arose for investigating and reducing the magnitude of this discontinuity as it may be responsible for loss of human lives. In an effort to understand and relieve effects of this discontinuity on risk management, a research project was started to define a generic framework that speaks to both engineering and operations cultures. It is important to understand that the two different cultures can never be fully harmonised, as the engineering culture is based on projects with clear start and end dates, while an operations culture is in essence cyclic in nature with no clear termination date at the onset of operations although there may be projects to manage change from time to time.

The real-world problem is thus the existence of a discontinuity in the acquisition of electronic safety equipment in mines, which leads to a discontinuity in the management of operational risk. The research problem can be stated as follows:

In the full life cycle of electronic safety equipment, a risk management discontinuity exists between acquisition and operational phases.

The shortfall stems from the differences in culture between engineering and operations and the lack of a unified acquisition process. From the research problem, a research goal that addresses the real-world problem, can be stated as follows:

Provide an abstract, generalised framework for an acquisition process for electronic safety equipment from a risk based, full life cycle system perspective.

Solutions to the stated research problem may differ, depending on the perspective of the individual that defines such a framework. Therefore, the perspective developed in this research will have a specific bias, namely an “operational” and “systems engineering” bias – this is not argued. Thus, the generic framework developed in this study provides an abstract view of equipment and its relation to operational risk with a distinctly pragmatic focus. That is, the acquisition process model is aimed at assisting risk analysts, engineers, and operations managers by providing a full life cycle view.

Whereas financial institutions (and similar disciplines) focus on modelling absolute, quantifiable risk, this research focuses on providing decision support information in the form of relativistic risk comparison in a trade-off. This is important as there are different ways to demonstrate the value of risk modelling. A relativistic approach allows the engineer to decide on functionality and resource definitions in the development phase (a function-focused approach), and allows the manager to understand the impact of resource selection (a resource-focused approach) on the risk of a system in operation.

Therefore, this research provides a view of risks associated with activities in operations, with the aim of providing defining an equipment configuration that is optimally designed for specific operations by using *activity-based risk analysis*, a definition that describes the methodology of this research clearly. The end result of activity-based risk analysis is equipment functional configuration, with the difference that the product has been analysed *in operations* as opposed to a product that has been defined by engineers and used by operations.

A distinct focus is on human performance variability, as this variability will be present in all operations that involve human operators. By including performance variability in operational models, sensitivity with respect to human performance variation is taken into account. This is done by using risk scores and volatility definitions that dictate decisions and actions taken by human operators in the system.

Chapter 2 provides a clear definition of the research approach that was followed in this research. Design science research is introduced and its application in this research is discussed. A process model is used to show research process inputs, constraints, enablers, and outputs, and knowledge contributions from this research are defined.

Chapter 3 analyses the research problem to provide a defined context for the research problem, and to validate the research problem as such. The research problem is translated to individual research challenges shown in a matrix. Matrices are used to assist in reading of this thesis and to provide traceability of the systematic conversion of the defined research challenges to a risk based acquisition process.

Chapter 4 gives definitions of risk terminology and discusses a framework selected for risk management. An overview of existing literature is given and the chapter summarises perspectives on risk from different research domains. These perspectives include (i) risk analysis methods, (ii) tools and techniques, and (iii) human error modelling that includes accident modelling. Systems engineering is discussed to provide a reference framework for a risk based acquisition process, with specific attention to the preliminary design phase. The chapter concludes with a traceability matrix that links research challenges to literature in order to validate both the research problem and the research solution.

Chapter 5 presents an acquisition process with a distinct risk perspective. The acquisition process is used to define the functional configuration of equipment in an iterative fashion. Application of this process to the acquisition of electronic safety equipment for mines is defined and presented in workflow format. Activity-based risk analysis is presented as a risk analysis method to be used in the activity-based risk acquisition process, as defined in Chapter 5.

Chapter 6 shows how activity-based risk was applied to the acquisition of electronic safety equipment for the case of an electronic winch signalling system. The case study took place over a number of years as development of actual electronic systems was done. The activity-based risk method was comprehensively applied, and fully

documented in Chapter 6, to arrive at two physical artefacts, namely a risk-reduced and a cost-reduced electronic signalling system. Both systems were evaluated by mines in controlled operational environments and authenticated and thus validated.

Chapter 7 provides a summary of the research results and shows how this research arrived at the concept of activity-based risk acquisition. The characteristics of the acquisition process and activity-based risk method are listed and discussed, after which verification and validation of this research are shown. The traceability matrices are used to show how the research challenges were systematically addressed.

Chapter 2
Research approach

2.1 Overview

This chapter defines the research framework applicable to this research. Design science research (DSR) is a research method aimed at solving real-world problems with the aim of not only performing an abstraction of the real-world problem, but also producing an artefact that has been subjected to a process of rigorous verification and validation. DSR forms the backbone of this research and is described in detail in this chapter. Also, a process block defining the inputs, resources, constraints and outputs of the research is discussed. The chapter concludes by showing how DSR was applied to this research and the contributions from this research effort.

2.2 Design science research

DSR is a problem-solving paradigm [1] that is suitable for directed research – that is, research that addresses an actual and current real-world problem. It can be described as a research approach with the focus on creation *("how things ought to be in order to attain goals, and to function"* [2]) and design (*"to change existing situations into preferred ones"* [2]) while the creation of an artefact (*"something created by humans, usually for a practical purpose"* [3]) serves as an outcome [4].

It is important to know that DSR is a research methodology that delivers both theoretical and real-world results. This is done by defining a real-world problem and translating this real-world problem into a research problem and theoretical framework inside which analysis and synthesis are done. The framework is used to analyse the real-world problem in a theoretical domain while adding knowledge to the knowledge base. Possible theoretical solutions to the problem are found from literature and inductive reasoning and are used to construct an integrated theoretical solution in the abstract domain. This theoretical solution forms the basis of a real-world solution, which is then subjected to a process of rigorous verification to result in a real-world solution that is validated. In doing so, the knowledge base is enriched and a usable artefact results from applying the DSR methodology. This concept is illustrated in Figure 1 on the next page [5] [6] [7] [8] [9].

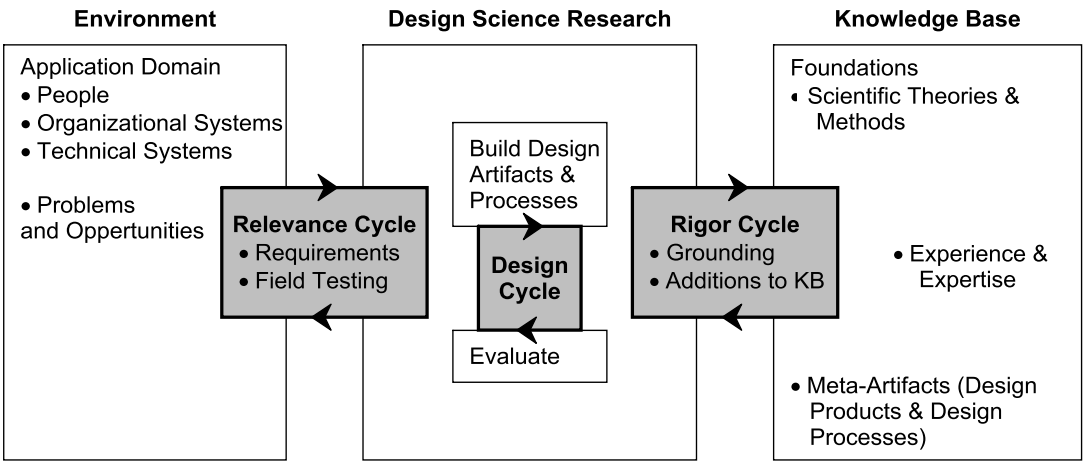


Figure 1: The design science research cycles [9]

The DSR framework that will be used during this research study is similar to a framework used for information systems as set out by [1]. In this framework, design consists of two entities, namely a process (set of activities) and a product (artefact). In the problem-solving paradigm, this view of design means that the perspective continuously shifts between the design processes and design artefacts for the same complex problem. Thus, the design process consists of a sequence of expert activities with the focus of producing an innovative product (the design artefact). After the artefact has been produced, the artefact must be evaluated. This evaluation provides feedback and a better understanding of the problem. This feedback is used to enhance the quality of the product, but is also used to improve the design process. This build-and-evaluate loop is iterated a number of times, after which the final design artefact is created. [1]

DSR produces two design processes and four design artefacts (as identified by *Smith* and *March* in [10] and confirmed by *Hevner et al* in [1]). The two processes are build and evaluate, as discussed in the previous paragraph, while the classification of the four design artefacts are as follows:

- Constructs provide the ontology in which problems and solutions are defined and communicated, thus the conceptual vocabulary of the domain;
- Models make use of constructs to represent an actual real world scenario. Models are used to address the design problem and its solution space;
- Methods consist of a set of steps used to perform a task;
- Instantiations comprises the operationalization of constructs, models and methods [7] [11].

In terms of this research, the design artefact consists of (i) a risk-based framework (instantiation) for the acquisition of electronic safety equipment, with a risk focus and (ii) the actual products used to address the initial need. The risk-based framework will consist of constructs, models and methods to form an integrated solution to the research problem, while the actual product is a set of functionally capable devices used to mitigate risk in deep mines.

2.3 Inputs, constraints, resources and outputs

To further explain the research process and define the research environment, an IDEF0 diagram of this research is shown below. Inputs to the research process are shown to the left, controls / constraints are shown at the top, resources and other research support are shown at the bottom, and outputs are shown on the right-hand side of the research process. The process itself is design science research (rolled out over time), as defined above, with a design and development centred research entry point.

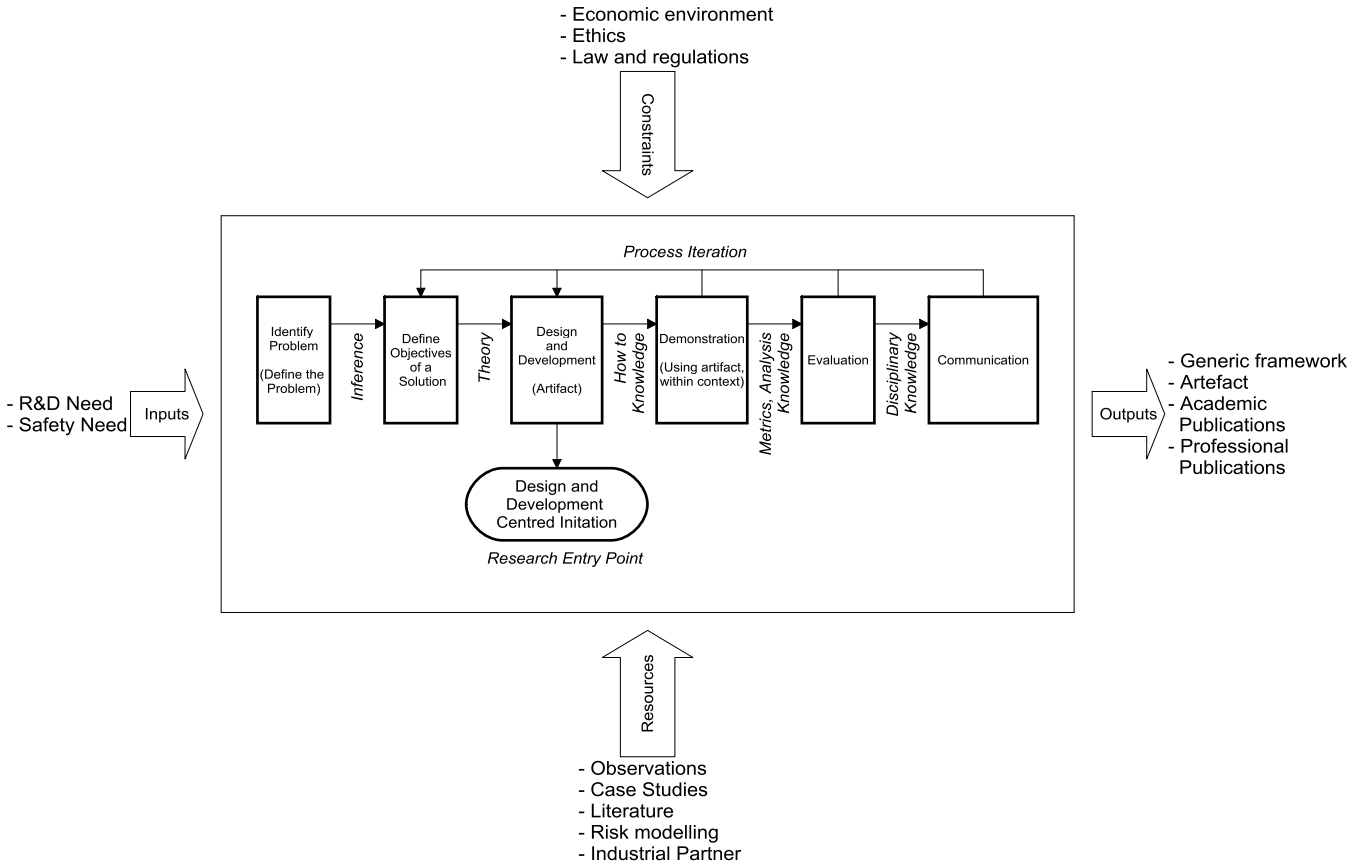


Figure 2: IDEF0 illustration of the research (modified from [5])

2.3.1 Research inputs

The main input to the design science research process is a real-world problem, namely the existence of a discontinuity in the definition and management of operational risk between the acquisition and operations phases in the mining environment. This input is based on observations from real-world projects.

2.3.2 Research outputs

The output of this research includes (i) a theoretical (abstract), generic framework for the definition and management of operational risk from a full life cycle perspective, (ii) a methodology for the application of this framework to real-world problems, and (iii) artefacts that provide evidence of the effectiveness of the framework and methods in (i) and (ii). In addition to the aforementioned research outputs, specifications for products (artefacts) emanated – these specifications are important for use in the acquisition phase of the supply chain.

Although the framework may be applicable to environments outside the mining industry, the real-world research was done based mainly on observations from the mining environment, and further research may be required to validate the model's applicability to environments outside of this scope.

2.3.3 Controls and constraints

2.3.3.1 Economic environment in the mining sector

Numerous (increasingly intensive) labour-related disruptions have been occurring in the SA mining environment over the past few years. This includes mainly workforce strikes and associated violence that prevents mines from operating. During these times, it was difficult to gain access to mining operations (i.e. visits underground and verification in controlled operational environments). Despite this ever-present constraint, it was possible to obtain all information required to conduct this study.

2.3.3.2 Complexity and flexibility of operations

Complex operational activities occur within the mining environment. The operations in the SA mining environment are also human resource dependent as limited automation has been done in deep mines (mainly due to labour pressure). Thus, job creation is one of the main drivers behind the lack of automation. The human volatility factor adds a further complexity and flexibility to the predictability of operations, which has a direct impact on safety. For this reason, this constraint is also the motivation for conducting this study, namely the significant presence of human operators in mining operations.

2.3.4 Resources and support

2.3.4.1 Observations from mining operations

The research group was involved in a number of development projects in which risk assessments were performed. It became evident that risk management was done by following a predefined process with specific focus on hazard analysis. Valuable information was obtained from observing the way in which risk was defined and managed during the development phase. Since both engineering and mining operations were involved, different perspectives were observed and further investigated.

From this retrospective analysis, the research problem was defined as outlined in Chapter 3.

2.3.4.2 Case studies

In the case study of importance to this research, the researcher played a role of active observer and developer. This case study was done as a real-world project with real-world artefacts resulting from the study. In this case study, operational risk was identified and mitigated by analysing potential solutions on behalf of a local platinum mine – this was done as part of the development of a winch signalling and safety system for a deep mine. Validation of this research was achieved when the mine safety committee and an authorised representative from the mine authenticated the mitigations, after which more than 6500 systems have been installed and have been in operation since. The *concept* for the operational risk framework was defined with focus on the acquisition phase. Extensive details on the case study appear in this document, where the theoretical framework that has been synthesised as part of this research is presented (Chapter 4 and Chapter 5) and applied (Chapter 6).

2.3.4.3 Literature study

The research of existing literature was done in two sections. The first section was to identify and analyse literature contributing to the existing mining environment and their views toward risk and safety. This literature was relevant to validate the observations from mining operations, as the literature as used to validate the research problem. These are all presented in Chapter 3 where the research problem analysis is presented.

The second part of the literature study (Chapter 4) comprises processes, techniques, models, and methods that were identified as being relevant to the research topic. This information was used to assist to derive and develop a solution to the research challenges stated in Chapter 3.

2.3.4.4 Risk modelling

A full life cycle approach was followed in modelling risk. This modelling forms an integral part of the proposed framework as it allows one to simulate real-world operations and its associated risk. This is of importance as the system functions and states, determined by unpredictable human interactions become complex. SIMIO, a process modelling tool, was used for the model development of a safety system as presented in the winch signalling case study. Also, an operational ontology is used, for example, using “hazardous exposure time” and “production loss” as high-level risk-related factors as opposed to using terminology that prevents understanding of risk in operations. The complete risk framework was developed and was evaluated as part of a case study, and is presented in this thesis.

2.4 Research knowledge contribution

The discussion on research (specifically DSR) so far has focused on the actual research process. In this last section, the research effort and outline of this work are placed in context by classifying the research in terms of its knowledge contribution and summarizing the above discussion in a diagram.

2.4.1 Knowledge contribution

Challenges often exist with the identification of knowledge contribution in the DSR framework. This is influenced by the nature of the designed artefact, the state of the field of the knowledge, and the audience to whom it is communicated. A further fundamental issue, as also stated by [11], is that nothing is really “new” as everything is made of something else or builds on some previous idea(s). To determine when something is really novel or has a significant impact to the knowledge base, a DSR knowledge contribution framework was presented by [11]. This framework classifies different types and levels of research contributions according to starting points from the research in terms of problem maturity and solution maturity. The matrix representing this framework is shown in Figure 3 on the following page.

Using this matrix from Figure 3, the knowledge contribution for this study was classified to fall in the top left quadrant of the matrix. Thus, a new (improved) solution to a known problem was addressed in this research. The solution maturity level is thus lower than the maturity level of the application domain, and this study thus has an “*Improvement*” research focus.

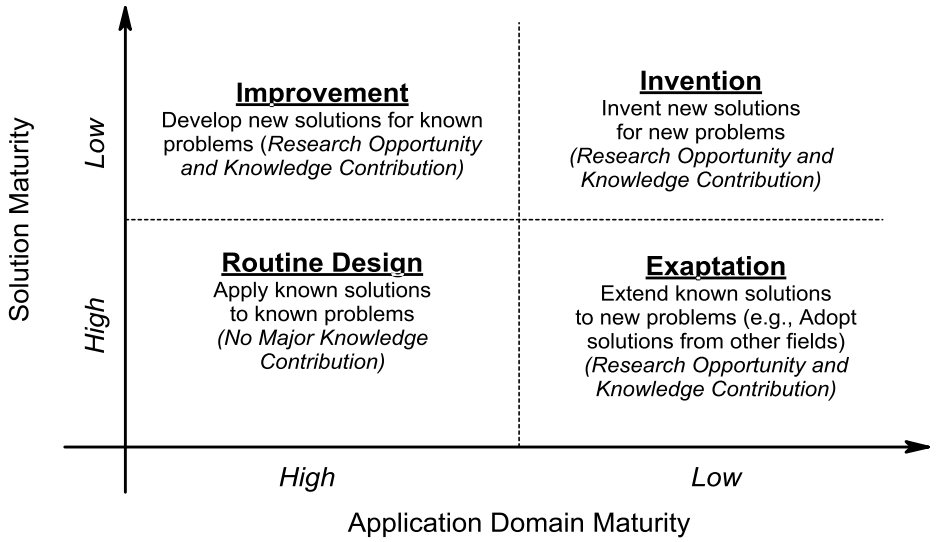


Figure 3: DSR knowledge contribution framework [11]

It is noted from [11] that the key challenge of the research type in this quadrant is the demonstration that the improved solution adds to the knowledge base. Due to this research challenge, the risk framework has been implemented in a real world case study where results with and without the artefact application have been evaluated. This forms part of the validation and verification section of this thesis, and is further discussed in Chapter 7.

2.4.2 Document outline in DSR context

The outline of this document is presented in Figure 4, where each chapter is shown to contribute to the overall DSR process. Chapter 2 (this chapter) provides a design science research framework and validates its application to operational research. This framework thus confirms that a structured research process was followed. Chapter 3 analyses and defines the research problem in detail – this is done to clearly validate the research problem as a valid research problem is a prerequisite for this study. A definition of research challenges is provided to guide the literature study and to focus the solution on relevant topics. Chapter 4 provides a literature study on operational risk and uses the research challenges from Chapter 4 as a guideline. The literature study thus provides more information on the abstracted problem and gives guidelines to be used in the design of a risk analysis method called activity-based risk, as explained in Chapter 5. Activity-based risk forms part of a larger risk management process to be followed as part of electronic equipment acquisition for mine safety. Chapter 6 makes use of a real-world case study of scraper operations at

the stopes, which is the area of concern inside a deep mine. Chapter 6 also provides verification that the risk analysis method applies to mining operations. Chapter 7 provides verification and validation evidence that (i) activity-based risk adds value as a method to analyse risk, and (ii) the products that were developed as part of this research are valid solutions for reducing risk at the stopes.

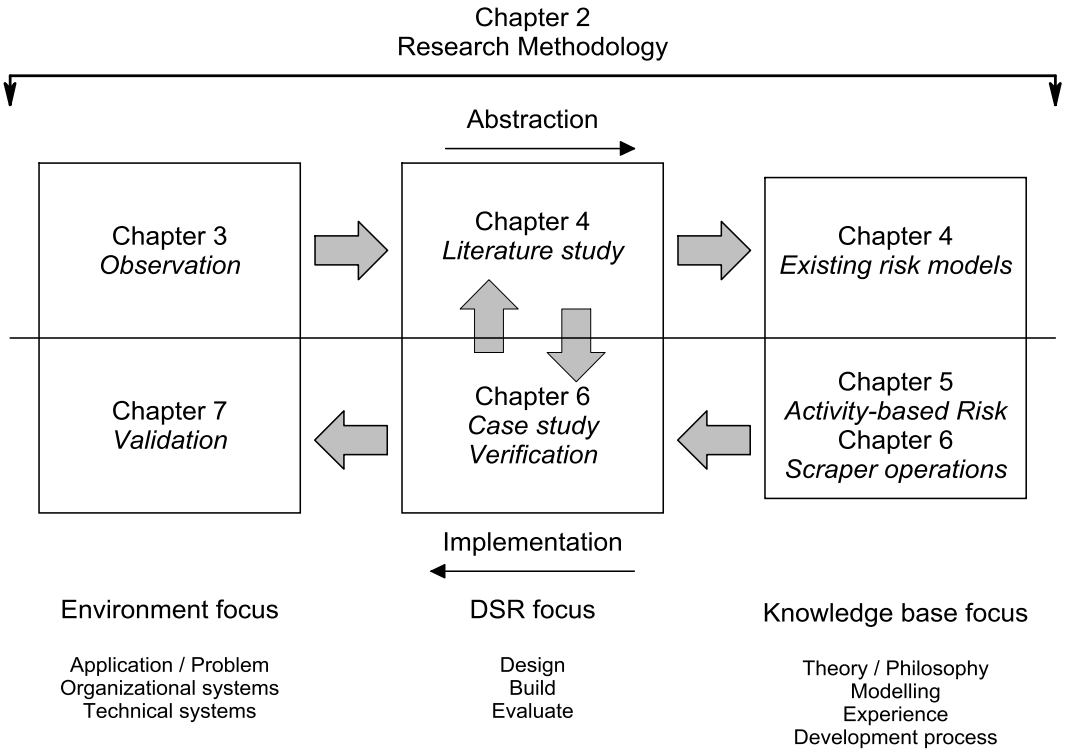


Figure 4: The document outline in the context of the DSR

2.5 Conclusion

This chapter presented the design science research (DSR) method used in this research. The DSR framework was explained in general, and the approach to this research was aligned with the DSR framework. Research inputs, constraints, resources and research outputs were defined using an IDEF0 process block, accompanied by a discussion on each element. The knowledge contribution for this research was classified to be "*a new improved solution to a known problem*". The outline of this document (and research) was finally presented within the design science research framework.

Chapter 3
Problem analysis

This chapter gives background on existing processes followed in the mining industry, specifically when new electronic safety technology is being acquired. At first, the risk management process from the Mine Health and Safety Act is discussed. A discussion on different hazard identification and risk assessment approaches introduced by SIMRAC (Safety in Mines Research Advisory Council) to the mines, as part of the risk management process, follows. To conclude the problem analysis, existing incident driven process observations are discussed, after which shortfalls and research challenges are presented.

Shortfalls relating to existing processes were identified from different sources, including observations during development projects and risk documentation from mines. The identified shortfalls were addressed in this research to develop a risk framework for the South African mining environment, with a specific focus on the development of electronic safety equipment.

As technology acquisition is an engineering function, formal engineering procedures exist that are used within the mining environment to mitigate and address the risks identified when accidents have occurred. This became evident from the Mine Health and Safety act together with risk management processes proposed by SIMRAC – these are discussed in the following two sections.

3.1 Mine health and safety (MHS) act

In the past, the focus of risk management in the mining sector has mainly been on financial risk. After the Leon-Commission of Inquiry, in conjunction with the UK regulation and ILO (International Labour Organization) conventions, have addressed this issue, the focus shifted towards risk management and mitigation in the management of occupational health and safety (OH&S). These recommendations were included in the Mine Health and Safety Act No. 20 of 1996 [12].

Section 11 from the mine health and safety act (29 of 1996) states that managers need to assess and respond to risk. During this assessment it is required to:

- Identify possible hazardous exposure;
- Asses these exposures to risk;
- Record the significant hazards identified and risk assessed;
- Records should be made available for inspection by employees.

It is further stated that all measures must be determined, in conjunction with the consultation of the health and safety committee at the mine, to eliminate or minimise any recorded risk by controlling the risk at its source. If residual risk remains, this needs to be addressed by personal protective equipment (PPE) and programmes to monitor risk exposures. These identified hazards and risks should be periodically reviewed.

This section of the MHS act also states that investigations must be conducted for every reported accident, the occurrence of a serious illness, and any health threatening occurrence. These investigations should take place in conjunction with the health and safety committee.

Upon completion of each investigation, a report should be produced as an outcome for submission to the health and safety committee. The report should contain the identified cause(s) of the risk event. Any identified unsafe conditions, acts or procedures that contributed to the risk event must also be stated, while recommendations need to be presented to prevent similar risk events [13]. This risk management process flow is further discussed and illustrated in Section 3.2.

It is further noted from the MHS act that there is a responsibility towards health and safety from the suppliers and manufacturers (or external contractors) of mining equipment, procedures, or designs. Section 21 of the MHS act states that [13]:

> *"Any person who designs, manufactures, repairs, imports or supplies any article for use at a mine must ensure, as far as reasonably practicable (i) that the article is safe and without risk to health and safety when used properly; and (ii) that it complies with all the requirements in terms of this Act*;"

Further details relating to this responsibility of the contractor are found in literature [13].

In the acquisition phase, equipment development contractors play an important role, especially in the development of new safety equipment. The responsibility of the mine and the contractor towards health and safety is of significance in this research as the research focus is on the acquisition of electronic safety equipment.

3.2 SIMRAC proposed processes

SIMRAC[1] (Safety in Mines Research Advisory Council), a supporting committee of the Mine Health and Safety Council, has conducted various research in the safety sector of the South African mining industry [14]. Given the results from the outcome of research projects, SIMRAC has proposed a generalised process to control the wide variation in content and quality of risk assessments. This process is documented in the *SIMRAC Practical guide to Risk Assessment* and is available to all SIMRAC levy paying mines [12].

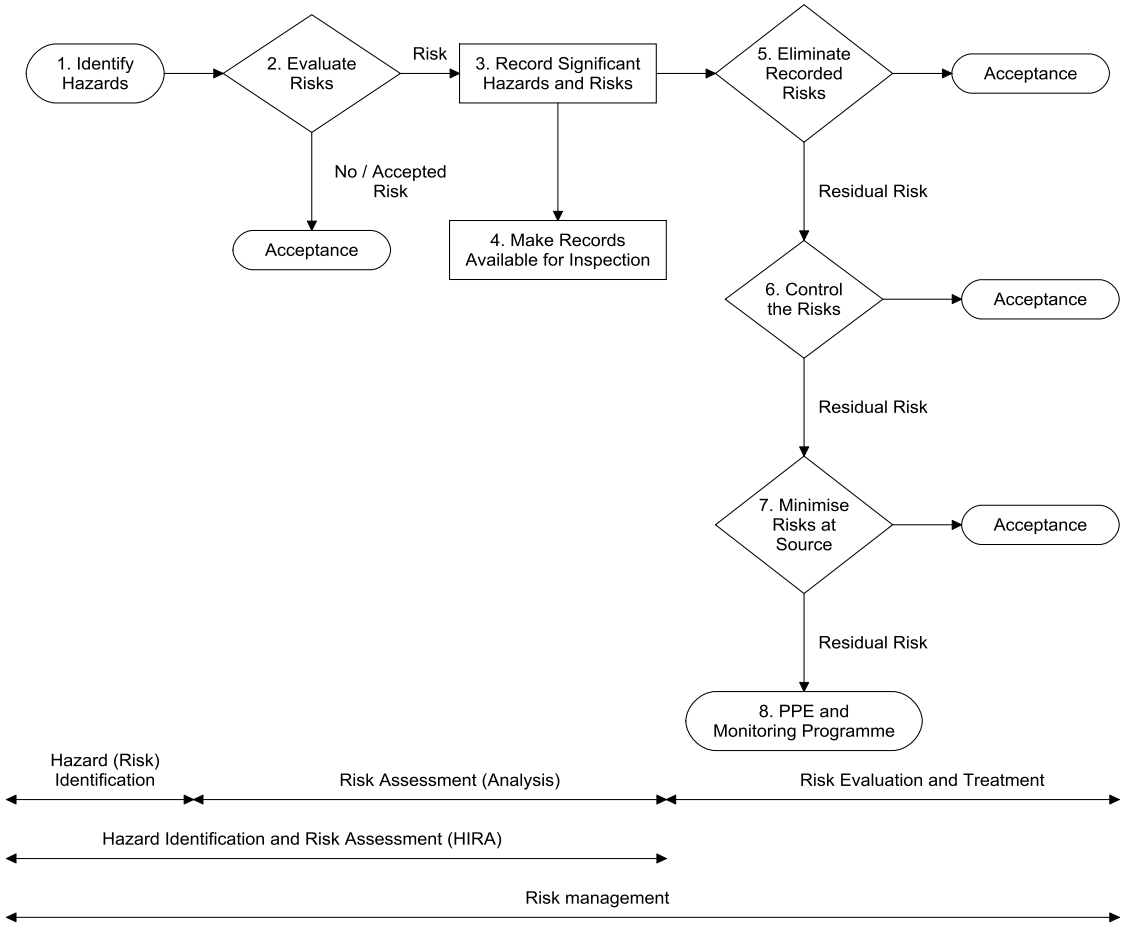


Figure 5: The risk management process [12] [13]

[1] Note: Although SIMRAC is no longer an operating entity, at the time of this research, prior research conducted by SIMRAC on safety in mines was found to be relevant to the mining environment. The duties of SIMRAC were taken over by the Chamber of Mines of South Africa (COMSA). This, unfortunately, left a need for a centralised knowledge base on safety, which is being addressed by this research.

The risk management process, as described by section 11 of the MHS act, is shown in Figure 5 above. This risk management process is divided into three sections, namely the hazard identification, risk assessment and risk treatment.

The primary objective of risk management is to assist an organisation to address identified OH&S risks. The focus of the risk management process is to determine ways and means to control the likelihood and impact of identified OH&S hazards, only after it has become evident that hazards cannot be eliminated in total, but can be mitigated (reduced) to acceptably low levels.

Outcomes from the risk management process specific to the mining environment are as follows [12]:

- During the risk management process, existing codes of practice, standards, rules, procedures, and work instructions are reviewed, and/or new practices are developed;
- This allows for the development of an outcome based education and training philosophy to OH&S;
- The risk management process allows for the review of the effectiveness of existing management systems;
- Compliance and progress is continuously monitored during this process [12].

Three types of hazard identification and risk assessment (HIRA) processes were identified which are used for risk management in the mining environment. These HIRA processes are all interrelated and form an essential part of the management system. The HIRA process forms only part of the overall risk management process as the HIRA process does not include risk treatment activities [12]. The three HIRA types are discussed in the sub-sections to follow.

3.2.1 Baseline Hazard Identification and Risk Assessment

The Baseline HIRA process is an initial risk assessment to provide a high-level establishment of risk profiles (or sets thereof) throughout the organisation. Each mine should determine the set of risk profiles most appropriate for the operation of that mine. Risks are mitigated according to priorities as set by risk profiles.

A typical example of such a risk profile established in the baseline HIRA process is shown in Figure 6. Risk quotients are shown in order of significance. A benchmark of the types and size of potential hazards that could have an impact on the whole organisation must be determined as part of this mapping, for example, winch operations in gulleys (as part of stoping).

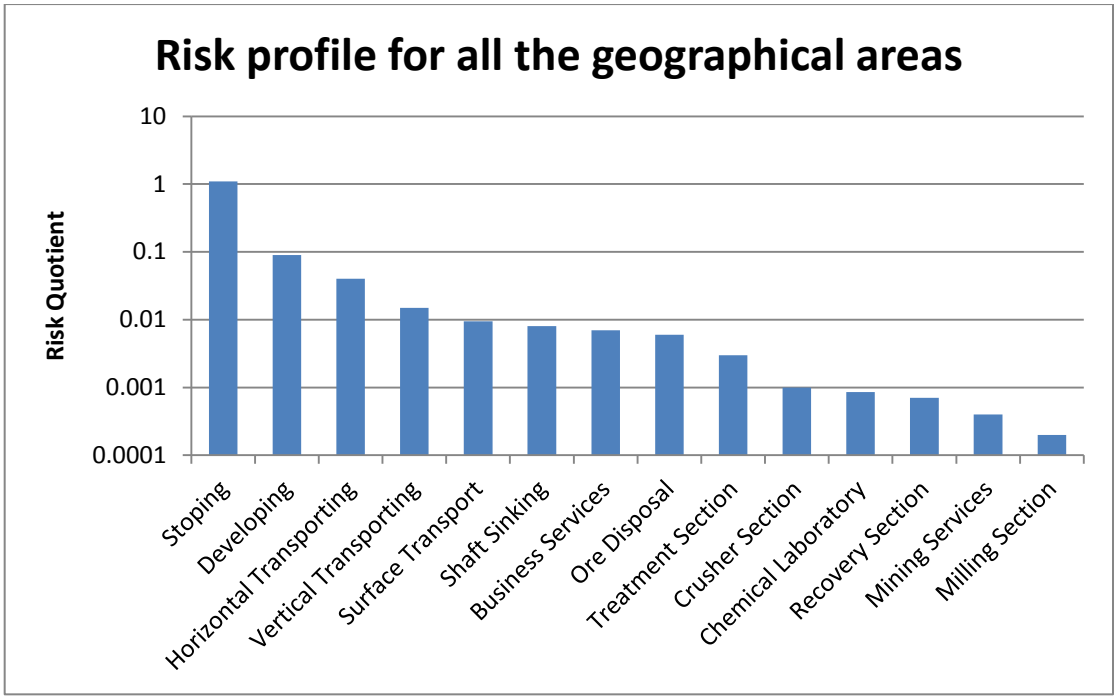


Figure 6: An example of a risk profile established during the baseline HIRA process (adapted from [12])

This HIRA process is normally reviewed annually to support business planning and budgeting. It should also be reviewed when circumstances have impacted a specific risk profile [12] [15] [16] [17].

3.2.2 Issue-based Hazard Identification and Risk Assessment

The issue-based HIRA process focuses on a detailed assessment study that results in the development of action plans for treatment of high risks. These should be clear, pragmatic recommendations to allow management to take action as stated by the terms of Section 11(2) of the MHS act. The risk profiles identified from the baseline HIRA form the basis for establishment of issue-based HIRA programmes [12] [15] [16] [17] . Issue-based HIRA is performed typically during the following activities:

- When significant accidents have occurred, or dangerous events occur;
- When new designs, new layouts, new equipment, or new processes are implemented;
- Specific findings that should be addressed during the continuous HIRA;
- Requests from employees;
- A change in the risk profile (from baseline HIRA);
- When new risk related knowledge and information become available.
- When requested from the DMR (Department of Minerals and Resources) or abnormal circumstances.

A generalised issue based HIRA process most often used in the S.A. mining environment is as follows *(the research team was also involved in this specific process during the acquisition of new equipment)*:

- Establish a risk assessment team: Individuals relevant to risk assessment are identified, typically across all organisational levels (operational, management, engineering, technical, health and safety, amongst others). Experience levels and expertise of individuals are important in the establishment of a risk assessment team;
- Conduct general discussions and determine possible solution: Once the team has been identified, a meeting must be set up where the scope of an issue must be discussed, during which relevant information must be identified. New equipment / technology may be suggested to address the raised issue, and a risk assessment must be conducted on the new solution (concept);
- Identify hazards and related risks: Team members must determine possible hazards and risks associated with the implementation of a new concept. The exposure of the mine – when employing new technology – is also determined;
- Define controls and their effectiveness: The risk assessment team must define controls to address identified hazards. These controls could typically be a process, a design change in the technology, or new technology. This alters the functionality of a conceptual solution / mitigation. Once all controls have been defined, the effectiveness of all controls must be determined and documented;
- Allocate risk scores: Risk scores are allocated to each hazard identified by the risk assessment team. These risk scores are determined in terms of a severity and likelihood and can be compared to the general risk scores of a probability risk assessment (PRA) approach. (This method is discussed in more detail in Section 4.3.)

3.2.3 Continuous Hazard Identification and Risk Assessment (HIRA)

The continuous HIRA process focuses on the following procedures:

- Identification of operational health and safety hazards with the aim to immediately treat the risk;
- Acquisition of information to feed back to the issue-based HIRA process;
- Acquisition of information to feed back to the baseline HIRA process [16].

In this day-to-day hazard and safety awareness process, typical tools such as inspection checklists, pre-use checklists, and critical part and path checklists can be produced as management controls. These are some of the outputs from the issue-based HIRA process.

The continuous HIRA process is performed on an operational level by operational floor management and first line supervisors. It is absolutely essential to perform the continuous HIRA process as the main emphasis is on “hazard awareness through hazard identification”. It is thus important to create a hazard awareness and safety culture in the organisation [12] [15].

3.2.4 The interrelationship between HIRA process types

Interrelationship between the three identified types of HIRA and management of the organization are described as follows:

- In the baseline HIRA process, issues that requires immediate attention are closely monitored through the continuous HIRA process;
- Outputs from the continuous HIRA process are used in the baseline HIRA process;
- Information acquired in the continuous HIRA process is further analysed in the issue-based HIRA process;
- Outcomes from the issue-based HIRA process must be monitored through the continuous HIRA process to ensure effectiveness and compliance of recommendations. This is typically done using checklists;
- Issue-based HIRA processes can be prioritised using risk profiles determined in the baseline HIRA process;
- Integrity and effectiveness of the risk management system are constantly evaluated and updated through the continuous and issue-based HIRA processes so that risk can be kept as low as reasonably possible;
- Baseline risk profiles should represent results from the complete risk management process. These risk profiles can be compared against previous risk evaluation cycles to determine the risk direction of the organisation [17].

The following principles are important in the HIRA processes:

- The process should be kept simplistic and practical – that is, pragmatic;
- The most appropriate risk identification technique should be selected based on the significance of the risk (see Section 4.4 for commonly used techniques);

- Transparency should be ensured and demonstrated throughout the proses;
- The most significant O&HS risks should be addressed first, according to priority;
- The risk management strategy as set by the MHS act should be followed;
- Aim to involve as many as practically possible employees during the HIRA process;
- Ensure contribution at all levels of employees, and do not treat inputs from low level employees as less important;
- Follow a systematic approach during the process [17].

The aim of this research is to develop an acquisition process model that fits into the above, existing risk management framework for mines. From literature and observations from involvement, it became clear that formal risk management procedures existed, but the primary risk focus was hazard based. Thus, risk measurement should include hazardous exposure to mine workers. In the existing framework "what" must be done to manage risk was clearly defined, but the "how" did not exist. Furthermore, a systematic approach should be followed in the acquisition process as it has to comply with safety and productivity, but limited systems engineering (SE) principles were evident in the existing framework as it focused on risk in isolation – Section 4.6 discusses SE principles in more detail.

The acquisition of electronic safety equipment must form part of the issue-based HIRA process as new equipment will be introduced or developed. A holistic, inclusive approach must be followed, taking into consideration the issue-based, continuous and baseline HIRA processes.

3.3 Observations on existing acquisition processes

Existing acquisition processes in the South African deep mining environment (typically gold and platinum mines) were used to form observations. This was done by participating in the risk management process as part of new technology development. Development projects include the development of scraper winch safety systems, horizontal vehicle collision avoidance systems, refuge bay safety systems, gas sensor systems and workplace illumination products. From this participation, it was observed that the current acquisition process is mostly incident driven. A typical model for an incident driven process is shown in Figure 7.

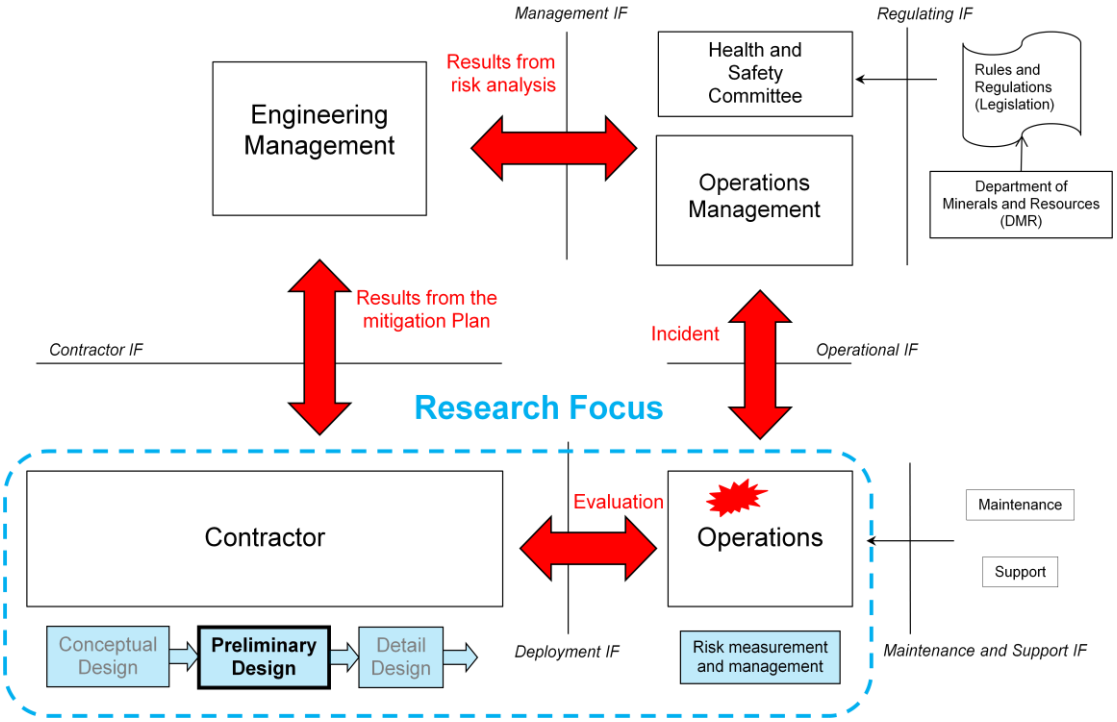


Figure 7: Observed incident driven operational process (from observation)

When an incident occurs during operations, it is escalated to management. Mine health-and-safety and mine management (operations and higher up) investigate and classify the incident. This investigation and analysis is regulated by various regulations including legislation form the DMR (Department of Minerals and Resources), the OHS (Occupational health and safety act) and MHS act (Mine health and safety act). The outcome of this investigation is typically an incident report containing a risk analysis. In some cases, frequently occurring incident types force the DMR to define legislation to prevent specific types of accidents.

High risks must be mitigated to prevent similar events / accidents. The mitigation is typically developed by using an engineering function and enforced by management. When engineering a new mitigation, risks are reviewed and further analysed, involving mining operations where necessary. This is typically done using the issue based HIRA process, as discussed in the previous section. The engineering management function will focus on the identification and / or development of technology / equipment to mitigate risk. The output of this process is generally a requirement specification for risk mitigating technology.

The requirement specification is typically provided to a contractor(s) to supply / develop the required technology. As the contractor is an independent body, and acts independently from the mine (and mostly in its own interest), the contractor function focuses on providing a verified product (which conforms to the specification), but

limited attention is paid (by the contractor) to validation of the product in operation. The contractor is sometimes considered the “expert” in providing the solution, which is partly responsible for a discontinuity in the full life cycle of the product.

Once the product has been developed and verified by the mine in a low-risk controlled environment, it is included in the mine’s standards. As observed, it is not uncommon for the risk impact on operations to only appear after deployment. As safety equipment generally has negative impact on operations (in terms of productivity), the solution is sometimes adjusted to address production needs. The results from this investigation are then used to amend the initial requirements set, which in turn is provided to the contractor to update / change the product / solution. This iterative evaluation process occurs until an optimised system has been developed and implemented.

This is a time-consuming process that may take months (and sometimes, years), during which miners remain exposed to the initial risk. It is also a costly process, as mines sometimes procure equipment that does not fully address all risks at first, implying costly changes during operation at a later stage.

3.4 Problem statement

The problem statement (from Chapter 1) is:

In the full life cycle of electronic safety equipment, a risk management discontinuity exists between acquisition and operational phases.

Shortfalls associated with the above discontinuity are identified and validated in this section, where each shortfall is translated into a research challenge to be addressed by this research.

3.4.1 Background and information sources

Given the background of the existing risk management processes (by observation though participation), the research problem statement was formalised. This was done from identifying shortfalls present in existing processes. The following sources of information were used in this analysis:

- Mine Health and Safety Act: This document states a typical risk management process, although insufficient detail is provided on how to implement such a process in practice;

- SIMRAC Documentation: A volume of research was done by SIMRAC on safety and risk in the mining environment. Sources include references [12], [18], [19], [20], [21], [22], [23], [24], and [25];
- Mining documentation: Risk management documentation from specific mines was made available to this research. These are high-level risk management procedures, and correlates with procedures and techniques from the risk management processes as described by [26] in ISO 31000:2000;
- Observations: Observations were made by the research team by participating in actual safety projects. These observations were made by taking part in the risk management process (as outlined above);
- Projects: The research team was involved in projects where electronic safety equipment was developed for the mines. These include:
    - Electronic winch signalling systems: Different functional configurations of electronic safety systems used in gulley scraping operations were developed and implemented (this project is also a case study that was integral to this research, discussed in detail in Chapter 6);
    - Horizontal vehicle collision avoidance systems: A radio frequency (RF) system was developed for underground vehicle collision avoidance. This system was risk analysed using the existing risk analysis process with additional analysis done using behavioural modelling;
    - Refuge bay safety systems: Safety systems were developed to provide refuge bay emergency indication, and were integrated with a SCADA system for status indication on surface. The mine's existing risk analysis process was followed;
    - Gas sensor system: A CO (Carbon-Monoxide) gas sensor system was developed for the refuge bay environment;
    - Workplace illumination: Different LED lighting technologies were researched and developed to allow for optimal lighting applications. Although not strictly a safety product, lighting is considered critical in stope environments. This project was done using the mine's existing risk analysis process.

In the projects above, the research team played the role of participating observer of the risk management process and played an active part in the development and implementation of electronic safety solutions. Thus, the research team was involved in a number of the acquisition projects for the development and implementation of electronic safety equipment.

3.4.2 Identified shortfalls

The shortfalls in the existing acquisition process were determined from an analysis of available literature and observations from projects and a case study, as described above. These shortfalls are stated as research challenges that were addressed in this research, as discussed below:

1. Detail requirements are not defined:
   It was found from both literature and observations that the preliminary design phase was absent (for all practical intents and purposes) in the acquisition process of new equipment. This includes the system functional flow (behavioural analysis), architectural design (functional building blocks and interfaces), as well as requirements and resource allocations. Design concepts are typically built and implemented without following a comprehensive preliminary design process to define the detail requirements of the system. This can result in major downstream problems in development, deployment and operational phases;
2. Sub-optimal safety technology is often implemented:
   Due the preliminary design phase being neglected, sub optimal technology is often deployed in operations. After the implementation of the first iteration of the development, it is often found that the end product does not really address the initial problem, or that the end product reduces productivity. Generally, it was found that where safety systems have a negative impact on mining operations (production) they were not accepted by end users and were consequently damaged or bypassed. The result is that development iterations are required, all tested in controlled environments, to determine a suitable solution, which had budget, time, resource and legal implications;
3. The focus is on hazardous exposure:
   In the existing process, risk analysis was done with a focus on hazard analysis. The result is that hazardous exposure to humans is determined, but the effects of production risk and technology risk are not considered (with regard to functionality, usability and reliability). These issues typically arise only after deployment of the technology;
4. Lack of integration and limited life cycle perspective:
   Mining operations, with a specific operations focus, is often not aligned with the engineering. As a result, technology is not integrated to its full extent for all phases of the full life cycle of the system;

5. The focus of risk assessments is mainly expert input and hazard based:
   When risk assessments are done, the integrity of the risk assessment result is determined by the experience of the risk assessment team. Although the team is of critical importance and must be used, there is a limited focus on the detail design of the safety system. Inputs from the team are documented, but often there is no systematic approach to guide the developer (often, the contractor) through the system design to ensure a comprehensive risk analysis is done. The current approach followed in risk assessment is mainly hazard based;
6. Reactive incident risk management approach is followed:
   After an accident has occurred, an incident is investigated – these investigations generally have a significant operational downtime as a consequence, particularly when fatalities have occurred. Safety systems are designed to enhance safety often only after incidents have occurred. Safety levels and associated mitigations should be determined more often and addressed proactively during the baseline HIRA and continuous HIRA processes to prevent safety and operational losses. When a “Section 54” (according to legislation, all operations must be suspended until an investigation has been completed) is enforced, production losses range from approximately R4M per day for a platinum mine shaft with 35 stopes and approximately R6M per day for a gold mine shaft of similar size. That is, platinum mines lose around R170k for a panel length of 30m, while gold mines lose around R240k for a panel length of 30m, with 70% of all panels blasted daily. These values were obtained in 2014 and will change over time.
7. Impact of specific technology is not measured using a common norm:
   In many instances, it is expected from suppliers to conduct a risk (hazard) assessment on new equipment (their own equipment, in many cases). Due to the lack of clear guidelines to assessors and the lack of an independent assessment, risk assessments’ quality varies between suppliers. This makes it virtually impossible to identify the product with the lowest “risk” score, as the same measures are not used across assessments. The supplier of technology is not aware of the exact operational conditions where a product will operate and often does not take productivity into account;
8. Lack of human integration in risk assessment:
   Observations showed that consideration of human performance variability was not evident in the risk analysis processes. The focus in a risk analysis is based on “*what the impact will be on the human*”, while the behaviour of

humans towards technology and the environment is not considered. Humans must be integrated in the evaluation of risk in an operational environment as their performance variability has the highest impact on risk.

The shortfalls above were addressed in this research. It became evident from the identified shortfalls that the design phase had to be improved (specifically, the preliminary design phase) while more focus should be on operations and human performance variability during acquisition, as indicated in Figure 7.

The identified shortfalls were translated into research challenges as shown in the top row of the traceability matrix in Table 1. Table 1 shows the sources of information on the left to show how information sources were used to validate the individual research challenges.

Table 1: Research problem validation

Research Challenges / **Information Sources**	Detail requirements are not defined	Sub-optimal safety technology often implemented	Focus is on hazardous exposure	Lack of integration and limited full life cycle perspective	The focus of risk assessments is mainly expert input and hazard based	Reactive incident risk management approach is followed	Impact of specific technology is not measured using a common norm	Lack of human integration in risk assessment
Mine Health and Safety Act	x		x		x	x	x	x
SIMRAC Documentation	x		x		x	x	x	x
Mining Documentation	x		x		x	x	x	x
Observations during Case Studies	x	x	x	x	x	x	x	x

Table 1 above shows research challenges of this research, derived from the initial problem statement. In the literature study (Chapter 4) the columns will be repeated, as a new traceability matrix is used to map literature study topics to research challenges. Solutions to research challenges are linked by using a similar matrix in Chapter 5 where a solution is proposed.

3.5 Conclusion

In this chapter the research problem was analysed by means of observations from projects and a case study performed in the mining environment. Literature, standards and risk documentation from mines were reviewed and used as additional sources of validation. This information was used to define shortfalls of the existing risk management process for new technology acquisition. These shortfalls were discussed and translated to research challenges. The research challenges were summarised in a traceability matrix in Table 1 and provide inputs to the literature study, where the research problem is further analysed and potential solutions are sought from available literature.

Chapter 4
Literature study

This chapter provides a study of literature relevant to this research. Literature from specific focus areas applicable to this research study is discussed in this chapter. This is done to further analyse the research challenges that were derived from the research problem definition in Chapter 3.

Specific focus areas and topics covered in this chapter are shown in Figure 8. This illustration indicates the use of information from research areas to transform research challenges into solutions. By first identifying and clearly stating research challenges, it is possible to systematically address each research challenge in a focused manner, after which solutions are formed by means of deductive and inductive reasoning. The relevant information of these research focus areas are discussed in the sub-sections that follow this introduction. This chapter concludes with a matrix that shows how each research area addresses the defined research challenges, and how solutions to these research challenges are constructed.

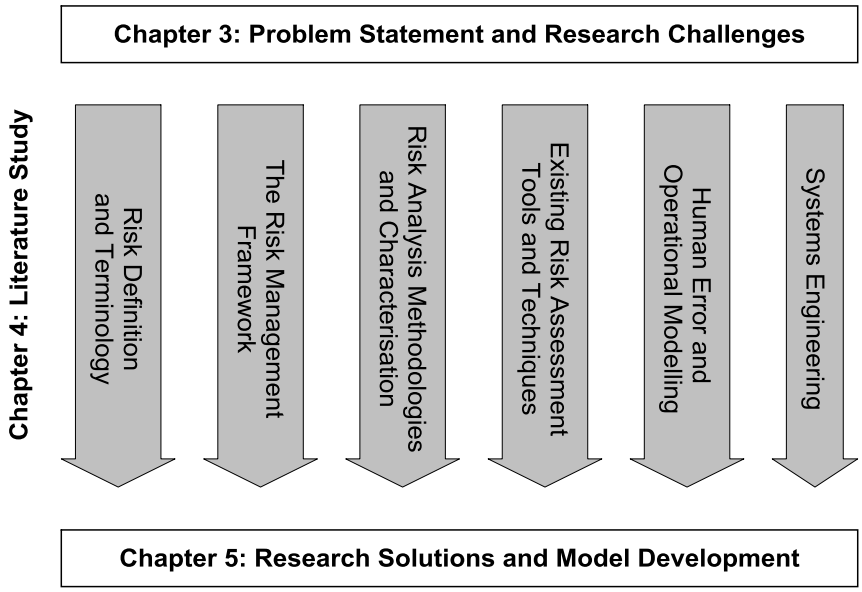


Figure 8: Literature study topics and focus areas

Please note that whenever a paragraph is printed in Italic font (cursive), the text is used to present deductions from literature, or to show relevance of literature to this research. This is done to clearly provide inferences and to simplify reading of this thesis.

4.1 Risk definition and terminology

Before proceeding to the detail of risk management processes, the concept of risk has to be defined in the context of this work. This concept, and its relevance to the research topic, is discussed in this section together with relevant terminology.

Many sources exist that define risk and related concepts (see [27], [28] and [29]). Risk terminology applicable to this study is discussed using EU,2000 [27], ISO/IEC 73:2009 [30] and ISO/IEC 51:2014 [31]. These guides are internationally accepted and present the most relevant concepts towards the risk framework of this study. Christensen *et al* [28] discuss and compare these concepts in further detail in their article where a common understanding towards risk is conceptualized across all industries.

4.1.1 Risk definitions

To form a comprehensive understanding of risk in the context of this research, three definitions of risk will be discussed from different sources. These are as follows:

1. Risk is defined by the ISO/IEC Guide 73:2009 (risk management vocabulary) [30] as "*effect of uncertainty on objectives*" where:
    - An *effect* is a deviation (positive or negative) from the expected;
    - *Uncertainty* is the likelihood of an event;
    - While *objectives* can have various aspects (financial, health and safety, etc.) at various organizational levels.

    It is observed that risk is often characterized as a combination of potential events (or their consequences) associated with the likelihood of the occurrence [30].

2. The ISO/IEC Guide 51:2014 (guideline for the inclusion of safety aspects in standards) [31] defines risk as follows:

    > *"A combination of the probability of occurrence of harm and the severity of that harm"*

3. The European Commission [27] defines risk as:

    > *"The probability and severity of an adverse effect /event occurring to man or the environment following exposure, under defined conditions, to a risk source(s)."*

These definitions express risk as a combination of:

- Probability of consequence/effect on the considered object (s);
- Severity;
- Extent of the consequence/effect.

Risk is defined under given circumstances [28].

The above elements of risk can be expressed in simplistic mathematical form as:

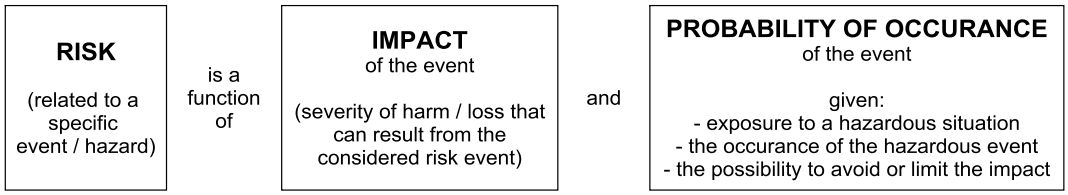


Figure 9 – Risk as a function of its elements [31]

This figure also represents the well-known mathematical equation used to represent risk:

$$R(risk) = I(impact) \times P(probability)$$

This risk equation is often used to quantify risk as part of a risk analysis process. This risk quantification is further discussed during the characterisation of risk in section 4.3.

It should be noted that an alternative (modern) view to risk also exists. In this modern approach, risk is a measure of exposure to loss at a level of uncertainty. Thus, exposure and uncertainty are required. For example, in this modern view where the probability of a loss is 100%, the level of risk is zero (because the loss is certain). This contradicts the traditional approach to risk where this scenario will typically result in a high risk [32].

During this research the traditional risk definition will apply as this is the risk concept used in the mining environment. Although the modern approach is more suited to the actuary and financial disciplines, it is still repeated in this document to avoid any ambiguity about this concept in this research.

The risk equation states that risk is a function of probability and impact of an event. Typically, in the mining environment, the impact of a specific event is fixed (if a person is exposed to the risk event) and cannot necessarily be mitigated – therefore the focus should be to address the probability of occurrence to limit the risk of a specific event. This risk probability is typically addressed by introducing electronic safety equipment in high risk areas, which in turn changes processes and user behaviour accordingly.

4.1.2 Risk terminology

Risk terminology applicable to this research is defined in this section. Definitions are repeated here to define the ontology of this research – that is, the environment in which this research has been conducted – as given below:

Hazard - A potential source of harm [31];

Hazardous event – An event that can cause harm [31];

Inherently safe design - Eliminating hazards or reducing risks by changing the design or operating characteristics of the product or system [31];

Residual risk - Risk that remains after risk reduction measures (protective measures) have been implemented [31];

Risk source - Agent, medium, commercial/industrial process, procedure or site with the potential to cause an adverse effect(s)/event(s) [27];

Risk analysis - A process consisting of three components: risk assessment, risk management (control) and risk communication [27]. However, risk analysis forms part of a larger risk management system, with the definition from [27] adjusted to also indicate risk control as opposed to overall risk management;

Risk assessment - A process of evaluation including the identification of attendant uncertainties, of the likelihood and severity of an adverse effect (s) /event(s) occurring to man or the environment following exposure under defined conditions to a risk source(s). A risk assessment comprises hazard identification, hazard characterisation, exposure assessment, and risk characterisation [27];

Hazard identification - Identification of a risk source(s) capable of causing adverse effect(s)/event(s) to humans or the environment species, together with a qualitative description of the nature of these effect(s)/event(s) [27];

Hazard characterisation - Quantitative or semi-quantitative evaluation of the nature of adverse health effects to humans and/or the environment following exposure to a risk source, or sources [27];

Risk characterisation - Quantitative or semi-quantitative estimate, including attendant uncertainties, of the probability of occurrence and severity of adverse effect(s)/event(s) in a given population under defined exposure conditions based on hazard identification, hazard characterisation and exposure assessment [27];

Risk management - The process of weighing policy alternatives in the light of the result of a risk assessment and other relevant evaluation and, if required, selecting and implementing appropriate control options (which should, where appropriate, include monitoring / surveillance) [27];

Safety - Freedom from risk which is not tolerable [31];

Tolerable risk - Level of risk which is accepted in a given context based on the current values of society [31].

The meaning of the word "***safe***" in the risk management context is often misunderstood. Some level of risk is inherent in most systems or products, as one cannot always be entirely protected from all hazards. Thus, the word "safe" in this context, does not mean that it is a state of being protected from all hazards. Instead, "safe" is the state of only being protected from recognized hazards that are likely to cause harm [31].

The risk concept and terminologies discussed in this section provides the context of the more detailed analysis procedures and methods to follow during this chapter and also further in this document.

4.2 The risk management framework

4.2.1 Generalised framework (ISO 31000)

This section provides a generalised risk management framework applicable to this research. The framework discussed in this section is commonly used in various international standards (ISO) [26] and literature [33] that relate to risk management in different disciplines where operational risk is present. The ISO 31000 standard is used as the primary reference for this section as this standard directly translates to the SANS 31000 standard (South African standard).

The risk management approach is illustrated at 3 levels, as shown in Figure 10 on the next page. The levels consist of the *Risk Management Principles* level (level 1), which feeds into the *Risk Management Framework* level (level 2). On the third level, the *Risk Management Process* is illustrated as used during the implementation of risk management.

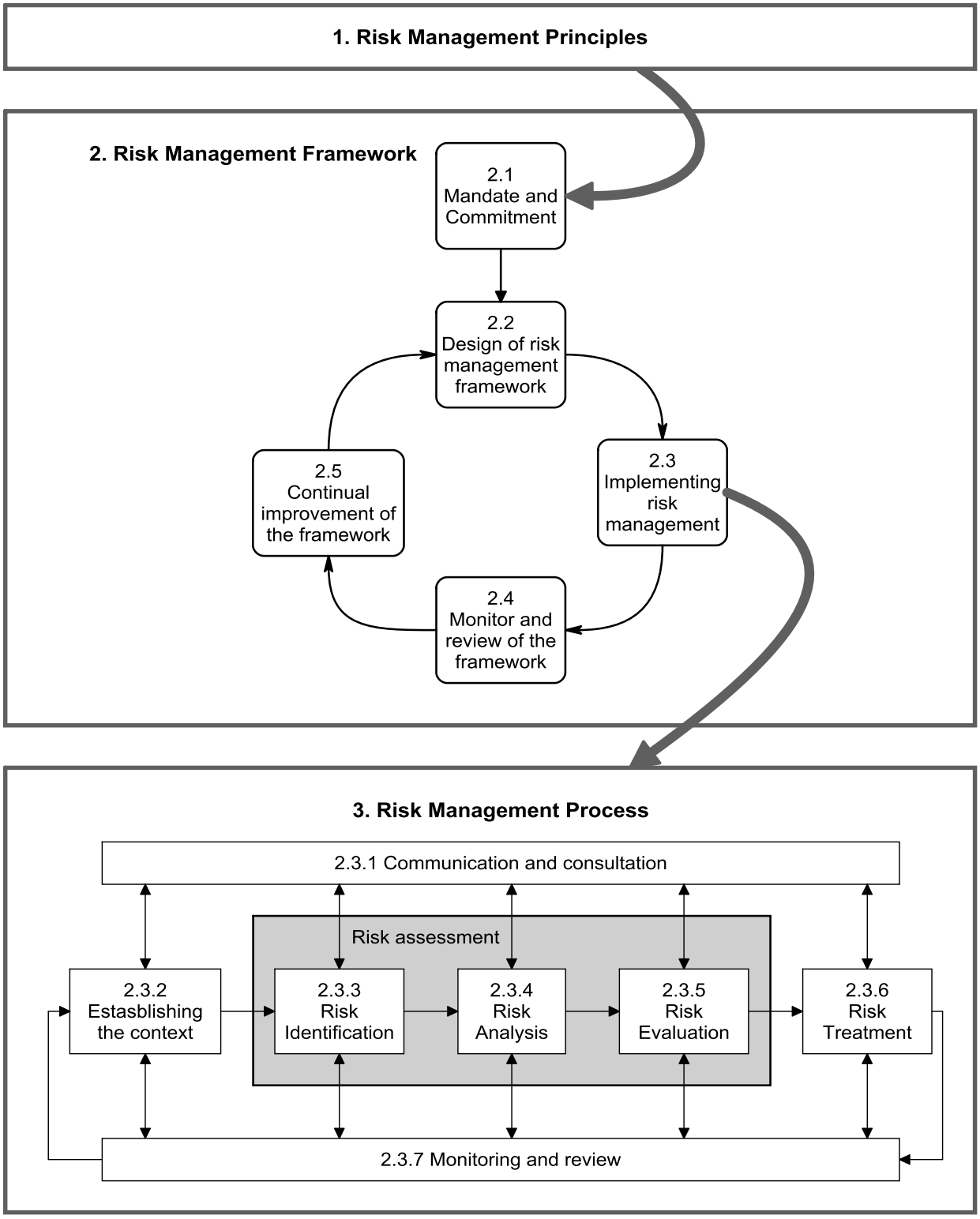


Figure 10: Generalised risk management approach [33] [26]

1. Risk management principles

During this study the focus is on the risk management framework and process – as the developed model and technique needs to fit within this process. The risk management principles that drive the risk management framework, as set out by ISO 31000 [26], is listed below:

- Creates and protects value;
- Is an integral part of all organizational processes;
- Is part of decision making;
- Explicitly addresses uncertainty;
- Is systematic, structured and timely;
- Is based on the best available information;
- Is tailored;
- Takes human and cultural factors into account;
- Is transparent and inclusive;
- Is dynamic, iterative and responsive to change;
- Facilitates continual improvement of the organization.

From literature, it was observed that the risk management principles as listed above provide general guidelines and do not directly address the research challenges of this study. Therefore, a risk management process was developed to address the research challenges as defined above, specifically applicable to the mining environment. The generalised risk management process as defined by ISO 3100 (and the MHS act) will still guide this research as a reference framework.

2. Risk management framework

The risk management framework above assists with management of risks when applied to different levels in an organization. The framework ensures that information from derived risks in the risk management process is effectively reported to relevant levels. This framework is also used as a basis for decision making and accountability at all relevant organizational levels.

This risk management framework is graphically represented in Figure 10. This framework assists an organization with integration of risk management with its overall management system. An overview of the iterative steps is described on the next page [26].

2.1 Mandate and commitment

To ensure the effectiveness of ongoing risk management throughout the organization, a strong and sustained commitment is required at the organizational management level.

2.2 Design a risk framework

The design and development of the risk framework for an organization includes the following:

2.2.1 A clear understanding of the organization and its context;

2.2.2 Establishment of a risk management policy;

2.2.3 Accountability, authority and appropriate competence for managing risk should be ensured;

2.2.4 The risk management should be integrated into the organizational processes;

2.2.5 Appropriate resources should be allocated for risk management;

2.2.6 Internal communication and reporting mechanisms needs to be established;

2.2.7 Communication and reporting mechanisms to external stakeholders needs to be established;

2.3 Implement risk management

The implementation of risk management includes the implementation of the risk management framework and its associated process as shown in Figure 10.

2.4 Monitor and review the risk framework

Risk management should periodically be monitored and reviewed to ensure effectiveness throughout the organization. Measurements include risk management performance relative to performance indicators and progress measures compared to a risk management plan. The actual risk must be reported, while the effectiveness of the risk management framework also needs to be reviewed.

2.5 Continually improve the risk framework

Action needs to be taken based on results from monitoring and reviews to introduce possible improvements to the existing framework. [26]

A clear distinction is made between the risk framework and the risk management process. The framework provides a generalized environment inside which risk can be managed, but the specific risk management process that must be followed depends on details of the organization and its characteristics. As a result, the risk management framework above applies to the mining environment in a general sense, but the specific process to be followed in a mine is the focus of this research.

3. Risk management process

The risk management process is illustrated on the 3rd level of the risk management approach in Figure 10. The process itself forms the focus of this study, which will be introduced on this level of the risk management approach. Each of the procedures within this process is described in the following paragraphs:

1. Communicate and consult

Communication and consultation with both internal and external stakeholders are required during each phase of the risk management process [33]. Communication forms part of the communication and reporting mechanism introduced in the design of the risk framework (see 2.2.7 of the previous section).

2. Establish the context

This phase establishes the risk management context inside which the process will take place. This includes the identification of basic parameters used for the management of risk to set the scope of the rest of the risk management process. The context also includes external and internal environments of the organization, with all interfaces between them. The outcome of this phase is to define the criteria against which risk should be evaluated and also the structure of the analysis. [33]

Literature that includes the international risk management standards [26] *and* [33]*, shows that typical activities of this phase include risk criteria development, internal and external context definition and the establishment of risk management context. Systems engineering principles with a specific focus on preliminary design, that should be present in this phase, was not specifically used in literature. It is imperative that a comprehensive preliminary design be executed to define the requirements of new technology that is introduced. In the preliminary design, the system architecture with system functions (behaviour) and all interfaces must be analysed. This preliminary design must not replace existing risk-related activities, but must be an additional activity in this phase to support existing activities.*

3. Identify risks

The risk identification phase determines a comprehensive list of sources of risks and events that may have an impact on each of the objectives specified in the context [33].

Risks should be included even if the source is not under control of the organization and also if the risk source or cause is not evident. This identification must include knock-on effects of specific consequences, including cascaded and cumulative effects. The wide range of consequences should also be considered. During this phase the identification of *"what might happen"* is typically done by working through identified scenarios to identify all consequences. All significant causes and consequences must be considered [26].

It should be noted that risk identification is the first phase of a risk assessment process followed by risk analysis and risk evaluation phases. This is also illustrated in Figure 10.

From literature, it is observed that comprehensive identification of risks in the risk identification phase is crucial because a risk not identified in this stage will be excluded for the remainder of the analysis [26] [33]*. This validates the research problem in that an effective risk identification technique is critical to the success of the process.*

4. Analyse risks

Risks are analysed to identify new controls and to evaluate existing controls. In this phase, the level of risk is determined by determining the consequence and likelihood of all risk events. This analysis must include the complete range of potential consequences and their mechanisms [33].

Well-known techniques and methods are available to perform the risk analysis as part of the risk assessment process - these techniques are discussed in more detail in Sections 4.3 and 0.

In the risk analysis phase, technologies must be included as part of the analysis to determine impact when using a specific technology or combination of technologies. Because different disciplines are present in a large system, it is not uncommon for risk to be analysed in similar fashion – that is, a segmented approach is followed. This research study will address this shortfall by employing an integrated approach, but also an approach where risk of each specific function (still integrated in terms of resources) in the system is analysed. This allows a designer to develop an integrated system by understanding the contribution of all of its elements in a functional manner.

5. Evaluate risks

The risk evaluation phase uses the outcomes from risk analysis to make decisions about future actions. These decisions include whether a risk needs to be treated or if an activity should be undertaken at all, and sets the priorities of risk treatments.

During evaluation, qualitative analysis methods are typically used to determine priorities and treatments based on levels of risk. These methods are discussed in Sections 4.3 and 0. Priorities can also be set on the basis of consequence alone.

As risk is always present and must be accepted at different levels of risk, the concept of *tolerable risk* was introduced. As discussed by *Sir Frank Layfield* in 1987 [33], individuals are prepared to tolerate some risks under circumstances in return for specified benefits. A common approach to tolerable risk is the ALARP *("As low as reasonably possible")* concept where risk is divided into three bands as shown in Figure 11 on the next page.

The upper band represents an intolerable region, whatever the benefits of the activity may be, and therefore risk reduction measures are essential at all cost. In the middle band, the ALRP principle is presented. Here the costs and benefits are taken into account and opportunities are balanced against potential adverse consequences. The lower band represents negligible risks, where the risks are so small that no risk treatment measures are needed [33].

The ALARP principle as illustrated in Figure 11 is specifically used for risks with significant potential health, safety or environmental consequences. The practicality of the ALARP principle is twofold. On the one end one needs to ask: "C*an something be done?"*, while on the other end the cost and benefit of the action or inaction needs to be considered. Here it is asked: "*Is it worth doing something in this circumstance?"* These two aspects must be balanced carefully to fit within the context of a risk management framework [33].

The ALARP principle has historically been applied to evaluate safety risks in the mining environment. In many cases, electronic safety equipment is used to address risks, but these systems are introduced at a cost. It is thus important to do a cost-benefit analysis to select an appropriate technology. The evaluation phase allows one to perform trade-offs between different integrated solutions. A method for determining the true effect of technology on operational gains and losses must be developed in this research.

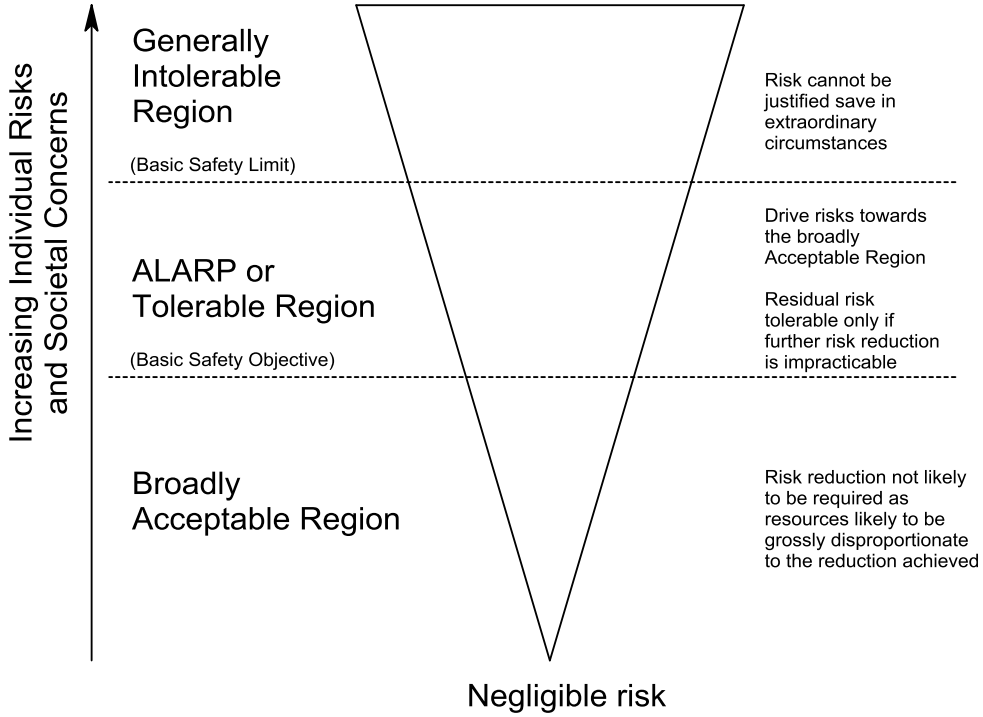


Figure 11: The ALARP principle for acceptable risk [33] [16]

6. Treat risks

In the risk treatment process, actions are performed as identified in the risk evaluation phase. Here treatment options are identified or developed to address selected risks. This is an iterative process as the treatment objectives must be evaluated to determine residual risk. If the residual risk is still not acceptable, further risk treatment plans must be implemented [33].

Observations from participation in safety-related projects underground revealed that risk treatment processes are sometimes implemented in operations while residual risk is being evaluated – that is, safety equipment is used while being evaluated. This introduces a new risk as an iterative process is followed to optimize technology in operation. Operations (and operators) are exposed to unknown residual risks during this process. A situation occurs where technology is introduced to reduce specific risks, but unwittingly, additional risks are introduced to the system. A method is thus required that performs trade-off studies before the introduction of new technology to operations. It is acknowledge that a reduced amount of adjustment will always take place after a technology has been introduced to operations.

7. Monitor and review

The ongoing review of risk levels and treatment strategies is essential to ensure the management plan remains relevant. Variations may be introduced at any time that may affect the likelihood and consequences of risk events. This also includes possible variation over time in factors that affect the suitability or cost of treatment actions. Typically, monitoring checklists are used to perform the monitoring and review function on a regular basis.

In this phase, lessons learned from following the risk management process must be analysed. This is done via reviews of events, treatment plans, and their outcomes. This data must be captured and made available for future use [33] as part of risk data.

This phase is important as it underlines the fact that risk management follows an iterative process. The process model developed in this research must include an iterative nature. The focus of the iterative component will be to reduce iterations in the operations phase – iterations should be allowed upon implementation of safety equipment under controlled conditions. It is appreciated that mines currently use a controlled test environment when evaluating risk in operations. Risks must still be monitored to ensure it is below acceptable levels.

4.3 Risk analysis methodologies and characterisation

Risk is characterised using methods as discussed in this section (characterised risk is an output of a risk assessment process). These methods typically focus on presenting risk as a meaningful risk value or in graphical format for visualisation purposes.

In the risk analysis process, events with more significant consequences and likelihood are treated with higher priority during the risk mitigation process. Risk mitigating actions include lowering the likelihood of an event, or reduction of consequences as far as possible should that event occur [34].

This section discusses qualitative and quantitative approaches commonly followed for risk analysis and characterisation.

4.3.1 Qualitative methods

Qualitative methods identify elements of risk (impact and probability) using descriptive terms for a specific scenario or event. These qualitative risk assessment methods are commonly applied and are relatively easy and less tedious as the probabilities and impact of risk events are identified in a broad and more general fashion. This provides a generalised understanding of comparative risk events and a risk matrix is used to separate events into classes.

A representation of a risk matrix using the qualitative method is shown in Table 2. This table describes the magnitude of all consequences (impact) and probabilities using assigned levels. In this table, descriptions from AS/NZS 4360 [33] are used to describe the magnitude of impact as insignificant (level 1), minor (level 2), moderate (level 3), major (level 4), or catastrophic (level 5). In a similar way, the probability levels are described as almost certain (level A), likely (level B), possible (level C), unlikely (level D), or rare (level E). The meanings of these descriptions, in terms of the various impact types and probability levels, must be developed within context.

The risk matrix incorporates a predetermined risk acceptance threshold. The matrix is used to provide a risk rating as an output, given a specific risk event, by reading across and down the risk matrix by using applicable impact and probability levels. A risk reading is used to classify a risk event and to prioritise treatment activities for each risk event.

Table 2: Qualitative risk matrix example [34]

		Impact level (I)				
		1 *Insignificant*	**2** *Minor*	**3** *Moderate*	**4** *Major*	**5** *Catastrophic*
Probability level (P)	**A** *Almost Certain*	A1	A2	A3	A4	A5
	B *Likely*	B1	B2	B3	B4	B5
	C *Possible*	C1	C2	C3	C4	C5
	D *Unlikely*	D1	D2	D3	D4	D5
	E *Rare*	E1	E2	E3	E4	E5
	Risk Rating	***Low***	***Moderate***	***High***	***Extreme***	

In the specific example illustrated in Table 2, 25 potential combinations of risk outcomes are shown, divided into 4 different risk levels – low, moderate, high, and extreme. These risk levels are then used to compare the risks of different events and set treatment activities and priorities accordingly.

Qualitative approaches to risk characterisation is best used as a quick, first level exercise where many complex risk issues exist. This process will screen the low risk issues to focus on the higher risk issues of the system.

However, shortfalls exist when the qualitative approach is compared to the quantitative approach. These shortfalls are as follows:

- Qualitative methods are imprecise;
- It is difficult to compare events on a common basis;
- Vague justification of weightings placed on severity of consequences (impact);
- Emotive labels effect risk communication;
- The risk outputs (level based) make it difficult to allocate financial implications [16] [34].

The qualitative method is a less comprehensive method as risk is only classified into levels, with the aim of determining high risk issues of a system. The use of this method is currently limited within the mining environment due to this lack of completeness, although it is still discussed as background to the following methods that are more commonly used.

4.3.2 Semi-quantitative methods

Semi-quantitative risk assessment approaches are used to address some of the shortfalls known in the qualitative approach.

The semi-quantitative process follows the principles of a qualitative process, but assigns values or multipliers to probability and impact levels. This may also involve multiplication of frequency levels with a numerical ranking of consequence. This result that the outcome of the semi-quantitative approach provides more detail on the prioritised ranking of risk, when compared to the qualitative approach.

An example of a semi-quantitative risk matrix is shown in Table 3. In this table the probability and impact levels have been assigned numbers that have been multiplied to represent a numeric description of risk ratings. It should be noted that the assigned values are not related to their actual magnitudes, but can the numeric values being derived for risk to categorise these in risk groups. This example shows extreme risks as risk ratings higher than 15, high risks for ratings higher than 10, etc. [34] [16]

Table 3: Semi-quantitative risk matrix example [34]

		Impact level (I)				
		1 *Insignificant*	**2** *Minor*	**3** *Moderate*	**4** *Major*	**5** *Catastrophic*
Probability level (P)	**5** *Almost Certain*	5	10	15	20	25
	4 *Likely*	4	8	12	16	20
	3 *Possible*	3	6	9	12	15
	2 *Unlikely*	2	4	6	8	10
	1 *Rare*	1	2	3	4	5
	Risk Rating (P x I)	**Low (0 – 5)**	**Moderate (6 - 10)**	**High (11 – 15)**	**Extreme (16 – 25)**	

The advantage of this approach is that it allows risk ratings to be based on derived numeric risk values. A shortfall of this process is that numeric risk values may not always reasonably represent associated risk of events.

The abovementioned shortfall can often be overcome by selecting values for probability and impact levels more in line with their relative magnitude (thus, not absolute measures). This is typically done by assigning likelihood values of, 1 for almost certain, and divide by 10 for each level, up to 0.0001 for a rare event. Similar, the impact value is set to 1 for level 1 (insignificant event), and multiplied by 10 for each following level up to 10000 for a catastrophic event. Such a matrix will show the risk values in a logarithmic form, adding more weight to higher risk events [34] [16].

Consequence tables can also be used for risk assessments to assist with communication of risk events to management, where the risk matrix would only summarise risks. In the consequence table, typical fields would be (for the mining environment): potential hazard; risk severity level; current control measures; inherent risk score; recommended actions; and residual risk score. By using this table, risk is determined before and after risk controls have been put in place.
Thus, semi-quantitative methods provide a general understanding of the comparative risk between risk events. It is fairly easy to use and is useful for comprehensive risk assessment procedures [34] [16].

Observation from taking part in risk assessment process in the mining industry confirmed that mines follow a semi-quantitive aproach in line with SIMRAC guidelines. To assist this process, risk assessment tables are used to set up templates. This allows a designer to determine initial risk and residual risk after treatment procedures have been proposed for each identified risk event. These risks are then summarised in the form of a risk matrix.
By using this technique, the designer can quantify risk events but a realistic representation of risk still remains a challenge – even with a logarithmic scale. For example, risk is influenced by the characteristics of end-users of a system (operators). Also, it is often seen that frequency and impact levels differ when different analysts assign values to likelihood and impact. This is typically due to a difference in views, background, experience and sometimes agendas of analysts. This observation that people influence risk decisions is not new ([35] *and* [36]*), but adds to the validation of the research problem.*

4.3.3 Quantitative methods

The focus of quantitative methods is to determine the impact of risk events in terms of specified values. This can typically be estimates of cost, number of fatalities, etc.
A quantitative risk assessment approach follows the general risk approach of deriving an expression for risk (the risk quotient) in terms of its likelihood and impact by assigning absolute values to the likelihood and impact. The estimates of likelihood of event occurrences are made in terms of event frequencies, and/or event probabilities. These estimates are done by using consistent measures, selected appropriately to align with the inherent nature of a system.
The risk quotient is used to characterise and compare risk events in order to identify the events that pose the most risk. The consequences are often expressed in financial terms to represent “expected cost” or “expected loss” of an event. Two specific quantitative methods will be further discussed in the following sections. [34]

4.3.3.1 Risk Maps

A risk map is a quantitative representation of a risk matrix, where the risk matrix is an output of qualitative and semi-quantitative risk assessment. An example of a risk map is shown in Figure 12. This risk map is a similar representation of the knowledge base of the qualitative examples in the previous sections.

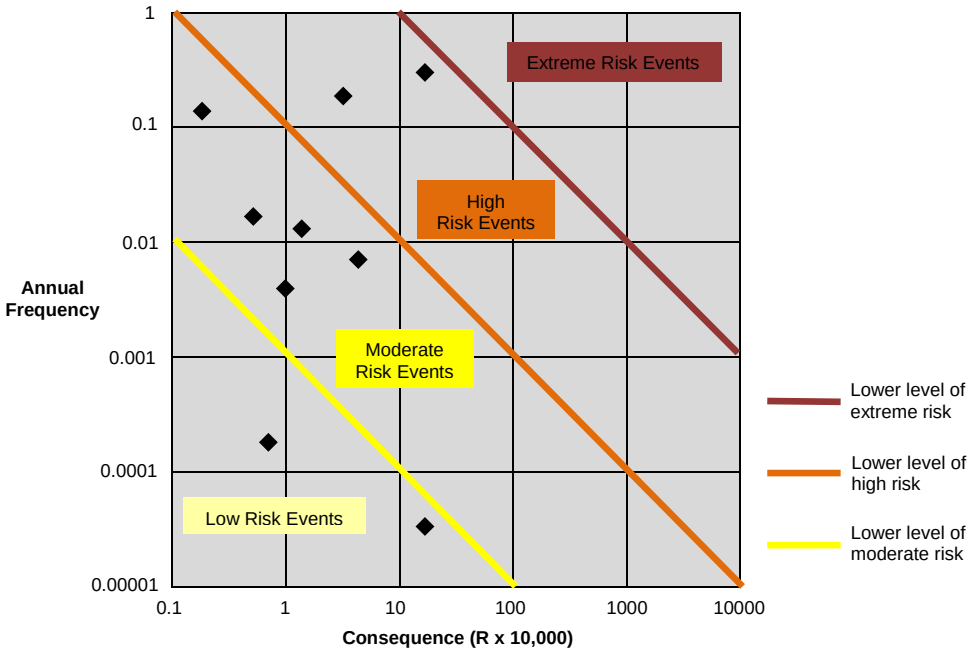


Figure 12: Risk map example [34]

A risk map uses consequence level and frequency of occurrence on the horizontal and vertical axes respectively. Risk severity areas are also defined on this map, allowing a risk analyst to determine risk levels of events.

Intervals of the axes (likelihood and consequence) increase by an order of magnitude. Therefore, diagonal lines on the graph represent lines of equal risk. The line representing the lower limit of extreme risk shows the risk quotient equal to a value of 10 along the lower limit. Thus, any point above this line will be an extreme risk event [34].

4.3.3.2 Risk profiles

Outputs of quantitative risk analyses are expressed in the form of risk profiles. Risk profiles were first discussed as part of the baseline HIRA process in Section 3.2.1, where the risk profile indicated the baseline risks for different sections in the mining environment. The risk profile discussed here includes high level economical factors (such as environmental effects, labour unrest, political factors etc.).

An example of another risk profile is shown in Figure 13, where risk characterisation is focused on specific risk events.

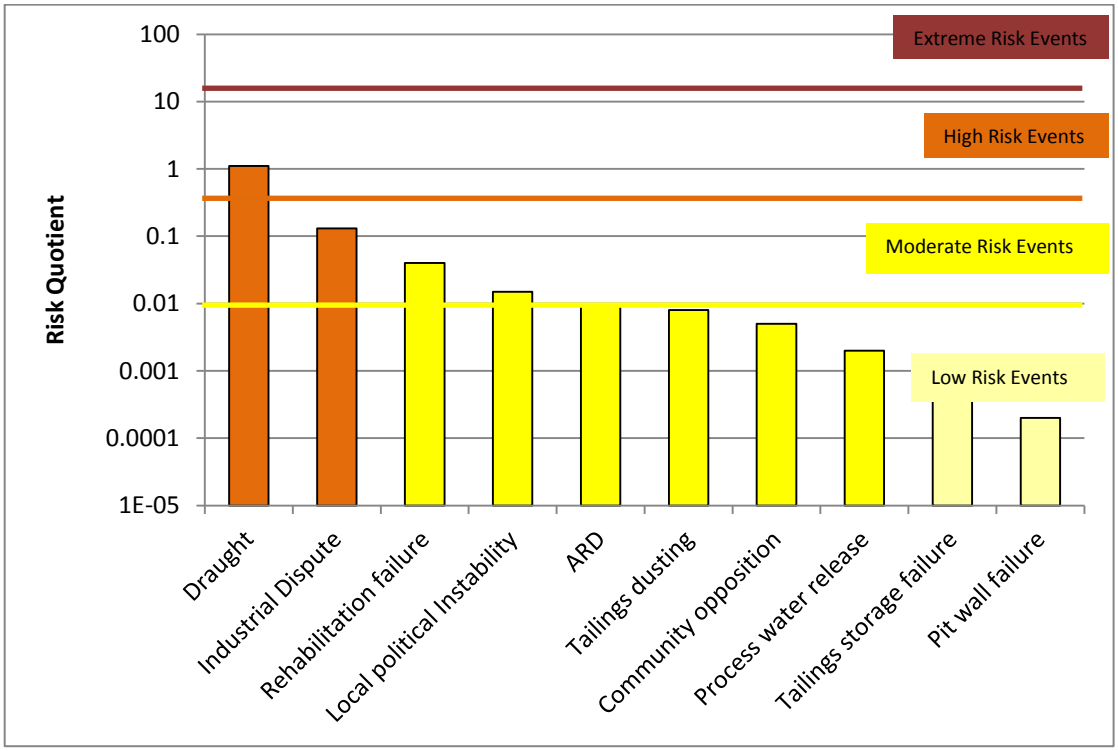


Figure 13: Risk profile example [34]

The example risk profile above shows a risk quotient for each potential risk event. Lower risk levels are indicated on the graph where risk quotients of all events can be relatively compared. The magnitude is presented on a logarithmic scale where, for example, the first risk event on the graph is estimated ten times higher than the second risk event. Risk events are arranged in order of decreasing risk, assisting the prioritisation of risk for later treatment.

Risk treatment strategies are assisted by adding decision support information to the profiles above, one of which is the exposure profile shown in Figure 14. This exposure profile indicates financial exposure (estimated cost) for each risk event, together with levels of conservatism. The risk quotient (depicted by the red line) in this figure correlates with that in Figure 13, but the financial exposure of events is on a linear scale. By using the visualization shown in this profile, a high risk / high cost event will be treated with high priority. The risk profile does not necessarily correlate with the exposure profile as the frequency of events are not taken into account in the exposure profile, whereas it is taken into account in the risk profile.

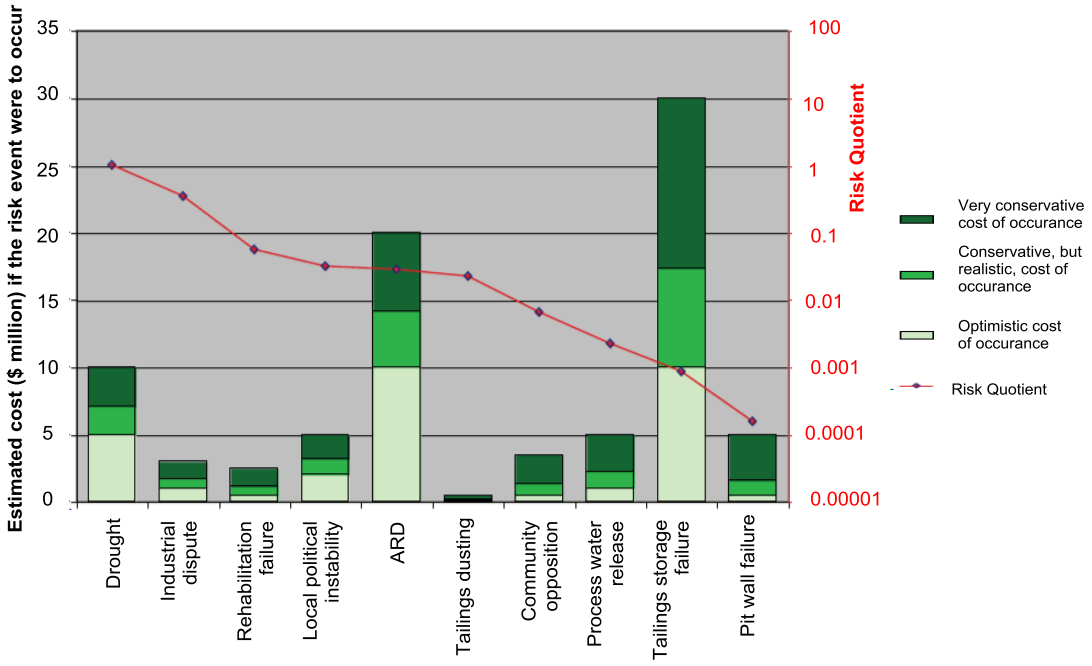


Figure 14: Exposure profile example [34]

Probability distributions of cost are shown in the example above in an effort to quantify the uncertainty associated with the impact of risk events. These calculations are typically done using simulation software that relies on Monte Carlo analysis techniques. Examples of software packages include @ Risk, Risk Solver, Risk AMP and Crystal Ball.

Variations in confidence levels of costs indicate the range of uncertainty associated with impacts of risk events. These confidence intervals are used to determine the type of action for risk events, where a smaller interval increases confidence and simplifies decisions on priority and treatment of risk events accordingly.

Financial decisions are also supported by quantitative risk assessment. This approach compares financial risks on an even basis with environmental and social risks while demonstrating transparency and consistency by following a logical approach.

Although quantitative risk assessment addresses many shortfalls of the qualitative approach, it is dependent on the availability of data and commitment from the organisation to manage the process and to employ individuals with adequate levels of expertise.

The quantitative approach is not recommended for environmental impact studies as people often do not accept the concept of placing a value (in terms of currency) on intangible and emotive events, including loss of life [16] [34].

Risk analysis in the mining environment is performed using a semi-quantitative approach. The cost associated with a risk event is sometimes measured in financial terms, which is not necessarily applicable to safety risk. Although there are significant financial losses evident when an incident occurs (when mining operations are suspended), it is not sensible to link those losses to a fatal loss as it is not possible to attach a monetary value to a person's life [34]*. When risk quantification is done in terms of fatalities (instead of monetary loss), it remains a challenge to translate injuries to fatalities, for example, how many broken backs are equivalent to death* [37]? *Although quantitative risk assessments are being increasingly applied in the mining environment, the process is often not intuitive and requires skilled and experienced decision makers* [35]*.*

The levels of conservatism presented by the exposure profile are of importance and are used to assist with model development in this research. This shows that volatility should be introduced in risk representation.

A quantitative risk analysis approach is further used in this research to introduce quantification of risk associated with acquisition of specific technologies. If one could quantify the risk in terms of hazardous exposure on the one end, and the production loss on the other end, the risk quotient can be used to evaluate different technologies on a relativistic basis.

4.4 Existing risk assessment tools and techniques

As illustrated in Figure 10, the risk assessment process consists of risk identification, risk analysis and risk evaluation. A risk matrix in its qualitative and quantitative forms is used mainly as a visualisation method. For a more in-depth analysis, a different tool set is required – the following sections provide information on specific risk assessment tools and techniques.

In this research, it is important to investigate existing risk assessment techniques to assist in the development of a new technique specific to the acquisition of electronic safety equipment in mines. Positive and useful aspects of existing tools and techniques are used to support the process model that is developed in this research.

A number of techniques exist for use in risk assessment as found from literature. These techniques include the use of the traditional methods, but many techniques were developed by adapting traditional methods to fit specific needs. In many instances hybrid techniques were created through combinations of more fundamental techniques, as discussed below.

In the section that follows, traditional methods are discussed, but all methods that were researched are listed for the sake of completeness. All relevant techniques and methods are discussed in detail, but less relevant techniques and methods are discussed in summary to preserve the focus of this research, namely that of operational risk. Traditional methods directly relevant to this research include Hazard and Operability Analysis (HAZOP), Failure Modes and Effect analysis (FMEA), Fault Tree Analysis (FTA), and Event Tree Analysis (ETA). More techniques are identified and listed after which the advantages and drawbacks of techniques are discussed in general.

4.4.1 Hazard and operability analysis (HAZOP)

The hazard and operability analysis technique is used to identify hazards in a system since hazards present themselves as probable risk events. This method typically employs a structured brainstorming session, involving relevant persons from an organization, to use their experience to determine possible and probable hazardous scenarios.

The HAZOP method is useful when a considered system involves humans with their behaviour, or hazards that are hard to quantify and detect. The drawback of the HAZOP method is that no provision is made for taking into account the cognitive ability of humans, i.e. why humans would commit unsafe acts. Also, the HAZOP

analysis method does not follow an integrated approach as the interactions between different components in the system are not taken into account. It can also be a lengthy, time consuming and expensive process [38] [39].

The HAZOP is a commonly used method in the mining environment to perform hazard identification to determine operational risk. Literature ([38] *and* [39]) *echoes observations from this research, as defined in the research challenges, that an integrated approach is lacking. The same holds for human cognitive factors, which are not always considered in an integrated manner in a HAZOP. Finally, a HAZOP process assumes that an optimal technology design has been carried out, as this is the basis of reliable HAZOP results. However, the preliminary design is often absent, which leads to a less than optimal technology design due to the absence of an integrated focus (an aspect of design particular to a comprehensive preliminary design phase).*

4.4.2 Failure mode and effect analysis (FMEA)

The focus of the failure mode and effect analysis is to examine individual components in order to identify possible failures of these components and their effect on the system. This method uses a forward (bottom-up), inductive approach to identify failure modes – i.e. components are deliberately failed to study downstream and upstream effects, as well as interdependencies as far as complexity of the system allows. The effects of potential failures are evaluated to allow recommendations and changes to the system to prevent unwanted failures and their associated risk events. The FMEA process is enhanced by listing all expected failure modes in terms of the use of the system, elements involved, mode of operation, operational specification, time constraints, and the system environment.

The steps in performing a FMEA are as follows:

1. Perform a system breakdown to define the system design;
2. Determine failure modes by identifying causes and effects of failure;
3. Rate the severity, likelihood of occurrence and likelihood of detection of each failure;
4. Compute a Risk Priority Number (RPN = Severity x Occurrence x Detection);
5. Implement corrective actions to minimize the occurrence of the more significant failure modes;

6. Re-assess the product or process by another cycle of FMEA after the corrective actions are implemented;
7. Review assessments on a regular basis.

It is recommended to perform a FMEA in the early stages of system design to ensure a comprehensive safety design. This also allows the designer to make changes to the system at a minimal cost. A drawback of this method is the emphasis on single failures (in isolation) of a system. It is known that additional hazards and risks result as a combination of hazards or events, but this combination of failure analysis is sometimes lacking approach due to combinatorial complexity. The focus of an FMEA process on an elementary (component) level is a concern as actual hazards may originate at a sub-component (lower) and sub-system (higher) levels due to interdependencies that are not always visible at component level only. Also, this approach does not readily incorporate failures that occur due to human error, as the focus is more towards the physical resources (technical equipment failures). An FMEA is a tedious (but necessary) process as a detail and structured analysis is of importance during the FMEA approach [38] [39] [40] .

Although an FMEA is a comprehensive process and can be used during risk analysis, this process lacks system integration and human-factor considerations as listed in the research challenges. FMEA must still be applied during the design of electronic equipment (low level) as the focus of this technique is on a component level. However, for the reasons noted above, it is imperative to address the research challenges with a method that uses the fundamental principles of FMEA but with additional integration and human factor considerations. Although the HFMEA (Human Failure Modes and Effects Analysis) method exists, this method focuses on low level human failures (thus, single-point failures [41]*) and does not consider the impact of interdependencies of failures.*

4.4.3 Fault tree analysis (FTA)

A fault tree analysis is an analytical risk assessment method and uses a top-down approach to identify failures that would have, or have had, negative impact on a system under analysis. The FTA method makes use of diagrams and logic relationships to indicate relationship between failures and events in a system. The aim of an FTA is to identify fundamental causes and impacts of hazards in a system by tracing failures through failure trees. The FTA method is thus mainly based on a root cause analysis principle, while visually illustrating cause-effect relationships between root cause events.

The steps in performing an FTA are as follows:

1. Define an unwanted event to study;
2. Obtain an understanding of the system to determine the cause and probabilities of the undesired event;
3. Construct a fault tree as follows:
    a. Each node in a fault tree is represented by a combination of preceding events that cause the unwanted event by using Boolean logic gates;
    b. Each gate is modelled with inputs (combinations) and outputs;
    c. An input can be a basic event or an output of another gate;
4. Evaluate and analyse the fault tree for any possible improvements.
5. Control identified hazards with the focus on decreasing probability of occurrence.

A fault tree method requires analysts to thoroughly study a system to prevent risk factors from being overlooked. An FTA, as currently applied to hazard analysis, falls short to fully integrate human error, mostly due to the complexity of human behaviour and the exhaustiveness of a tree analysis. An FTA is a time consuming, but necessary, method to support risk analysis [38] [42].

Although the FTA method is commonly used and one of the best tools available for comprehensive analysis, it does not detect all failures related to human failure. This method highly depends on reliability and failure data of components as combined in a fault tree. It is mostly complexity and lack of human integration that prevent this method from being a sole candidate to resolve the research challenges. However, valuable insight is gained from using this method as it allows a top-down (integrated) philosophy to some extent by linking higher and lower-level events through a fault tree.

4.4.4 Event tree analysis (ETA)

The event tree analysis method consists of a bottom-up method to identify and evaluate possible outcomes of lower-level risk events. The analysis starts by defining an initiating failure event and proceeds by evaluating every possible outcome that can result from such an event – these are presented as paths in an event tree, opposite to paths in a fault tree. Scenarios that lead to accidents can be evaluated in each path while considering safety constraints.

The steps to perform an ETA are as follows:

1. Define the system by selecting system boundaries;
2. Identify accident scenarios by analysing the system;
3. Identify initiating events (by performing a hazard analysis);
4. Identify intermediate events – that is, events that follow initiating events;
5. Construct an event tree diagram that represents all possible event paths;
6. Obtain event failure probabilities from statistics or probabilistic modelling;
7. Calculate the overall probability of event paths and determine risk;
8. Evaluate the risk of each path and determine its acceptability;
9. Recommend corrective action (when outcome risk path not acceptable).

The event tree method is easy to learn and implement, and incorporates interaction between the human, machine and environment. The drawback is that this method often focuses on isolated events as only one initiating event is considered at a time. When multiple initiating events are considered, different trees will be established, resulting in time consuming and lengthy analysis [38] [43].

The event tree method is of importance to this study as it supports the notion of integration of multiple elements with multiple initiating events. Complexity needs to be dealt with, but the event tree analysis, due to its logical and systematic approach, can be integrated with a normal operational analysis (more specifically, the flow of tasks).

4.4.5 Additional methods

A variety of additional methods exists for risk analysis. In a study done by *Marhavilas et al* [44], risk analysis and assessment methodologies were classified and compared using relevant scientific literature from the period 2000 to 2009. In this study, a variety of techniques were identified from more than 400 publications and categorized in 18 categories.

In a study done in 2002 by *Tixier et al* [45], 62 different risk analysis methodologies were identified from literature. In this study, the methods were reviewed and grouped into classes to indicate qualitative, quantitative, deterministic, probabilistic or combined properties of each method. This study was reviewed in 2007 by *Arunraj et al* [46], where these methods were further evaluated for risk-based maintenance purposes. The techniques identified and characterised from these two sources are shown in Table 4 on the next page.

Table 4: Classification of risk assessment methodologies [45] [46]

Method Types	**Deterministic**	**Probabilistic**	**Deterministic and probabilistic**
Qualitative	• Action error analysis; • Checklist; • Concept hazard analysis; • Goal orientated failure analysis; • Hazard and operability (HAZOP); • Failure mode effect analysis (FMEA); • Human failure mode and effect analysis (HFMEA); • Human hazard operability (HumanHAZOP); • Hazard identification system (HAZID); • Master logic diagram; • Optimal hazard and operability (OptHAZOP); • Plant level safety analysis (PLSA); • Preliminary risk analysis; • Process hazard analysis (PHA); • Reliability block diagram (RBD); • Task analysis; • Whatif? Analysis; • Sneak analysis; • Risk matrix.	• Delphi technique; • Expert judgement; • Rapid ranking.	• Maximum credible accident analysis; • Safety culture hazard and operability (SCHAZOP); • Structural reliability analysis (SRA).
Quantitative	• Accident hazard index; • Chemical runaway reaction hazard index; • Dow's chemical exposure index (CEI); • Dow's fire and explosion index (FEI); • Fire and explosion damage index (FEDI); • Hazard identification and ranking (HIRA); • Instantaneous fractional annual loss (IFAL); • Reactivity risk index (RRI); • Safety weighted hazard index (SWeHI); • Toxic damage index.	• Event tree analysis (ETA); • Fault tree analysis (FTA); • Petri nets; • Probabilistic fault tree (PROFAT); • Fuzzy fault tree analysis; • Risk integral.	• Method organised systematic analysis of risk (MOSAR); • Quantitative risk analysis (QRA); • Rapid risk analysis; • Probabilistic risk analysis (PRA); • International study group on risk analysis (ISGRA); • Optimal risk assessment (ORA); • IDEF methodology.
Semi-quantitative	• Domino effect analysis; • Layers of protection analysis (LOPA); • Predictive risk analysis; • World health organization (WHO); • Risk priority number.	• IAEA-TECDOC-727; • Maintenance analysis; • Semi-quantitative fault tree analysis; • Short cut risk assessment.	• Safety analysis; • Failure mode effect and criticality analysis (FMECA); • Facility risk review (FRR).

The classification of techniques shown in Table 4 indicates the wide range of research done on risk assessment processes. These techniques are not all discussed in detail, and relevant literature from [45] and [46] can be consulted for more information.

4.4.6 Observations and recommendations

It is evident that research has been done on a wide spectrum of risk assessment methodologies and techniques. Advantages and disadvantages of these methodologies and techniques were identified and will be discussed in this section.

In a research study done by *Renn* in 1998 [47], the strengths and weaknesses of each risk analysis approach were determined in an attempt to integrate risk assessment and risk perception. *Renn* states that risk assessments has become a routine operation for evaluating different hazards, chemical agents, or technologies and that these routinization may obscure the conceptual foundations and limitations of the methods and may further induce a false degree of certainty when dealing with potential side effects of human actions and interventions. It is further noted that technical assessments provide the best risk estimate when determining the probability of an adverse effect linked to an object or activity [47].

In a study done by *Sterling* in 1999 [48], the need for better communication, management and analysis during the risk assessment process were identified. In this study, trends and methodologies were identified with associated weaknesses. The outcome of this research provides key emerging themes that can be applied to further risk assessment approaches – relevant outcomes are listed below [48]:

- Unravel the different dimensions of the risk assessment problem and treat them as individual criteria;
- Ensure full consideration of uncertainty in the treatment of the technical aspects of risk estimation;
- Use the most simplistic and transparent techniques to express technical performance data and priority weightings on different risk criteria;
- The risk assessment focus should be on the systematic exploration of sensitivities;
- Focus attention on the construction of portfolios of technology and policy options, rather than choosing a single “least risky” option,
- Perform the risk assessment exercise as an iterative process rather than a discrete analytical act [48].

From this study, key properties of an enhanced risk assessment methodology are mentioned. These include the use of a systematic approach together with the disaggregation of the dimensions of risk, which will be addressed in this study by using systems engineering principles (see Section 4.6). Techniques should be simplistic and should have an iterative component to perform optimisation. It is

further noted that one should not shy away from introducing technology, as this is often the case when technology is introduced (technology adds complexity to systems that results in managers limiting its use). Technology does result in more complexity, but when implemented with caution, should in fact reduce risk up to a break-even point.

Backlund and *Hannu* have done a comparative study in 2002 [35] where three independent risk assessment techniques were performed by different consulting companies on a specific hydro-power plant. The outcomes from the assessments showed major differences in the performance and results from the analysis – all done on the same plant. The major factors identified in this study that contributed to the effects of different risk analysis results is (1) a vague requirement specification, (2) lack of systematic preliminary hazard analysis, and (3) incomplete documentation of the analysis performed. These factors that affect the quality of risk analyses are illustrated in the Ishikawa cause-and-effect diagram as shown in Figure 15 and discussed in detail in the reference [35].

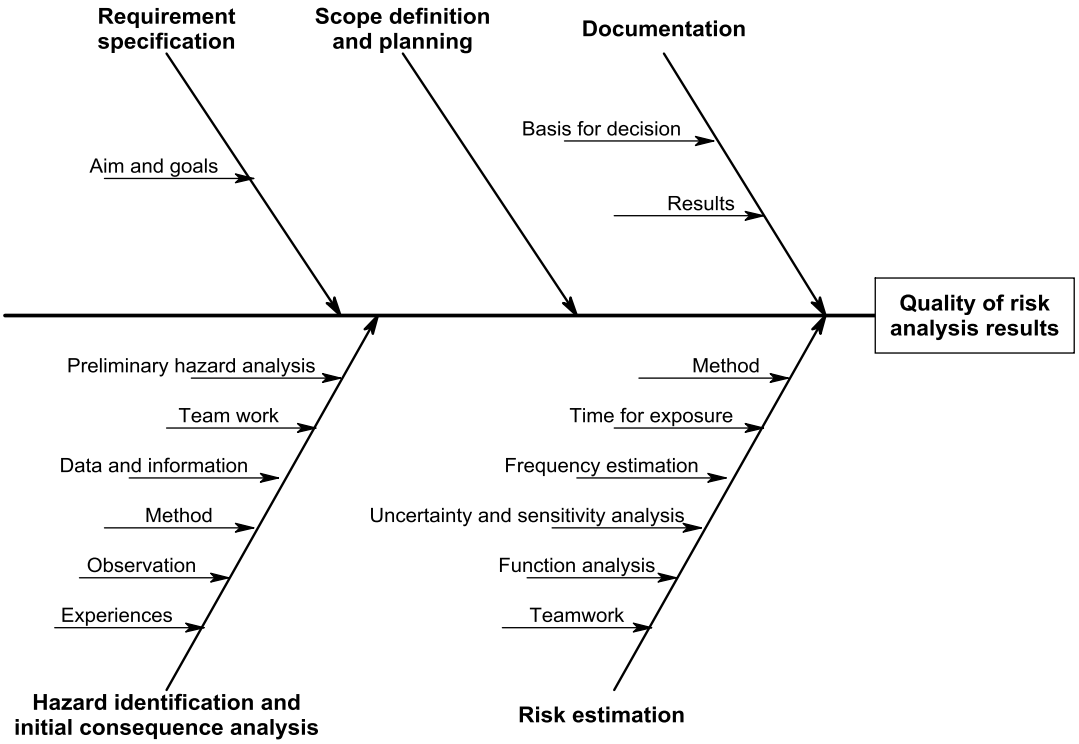


Figure 15: Factors affecting the quality of risk analysis results [35]

It is further concluded by *Backlund* and *Hannu* in [35] that desired functions of a system are of critical importance as these are the main reason why the system exists. Thus, the focus of performing a risk analysis should be on the functions required by the associated sub-systems or equipment (requirement) [35].

The factors and outcomes identified in the study above correlate with the research challenges, as observed and identified by the research team for the mining environment. Although the research problem was defined within the boundaries of the South African mining environment, literature confirms that these challenges are present in most domains where risk management is performed. The concluding remarks of [35] *address the research problem directly as this is one of the fundamentals of this research study – namely to optimise the system (or equipment) functions to ensure that correct technology is acquired. Quite often, the problem has been clearly identified (typically originating from a loss event in operations), but development requirements to the solution are unclear – this research challenge is confirmed by* [35]*. The result is that requirements are often developed in a limited, one-dimensional way without expert technical inputs or consideration of different technologies. To address this shortfall, the approach to acquisition introduced in this research study will provide a comparative, iterative approach to determine required system functions that directly address hazardous exposure and production time lost (performance measures that directly translate to risk) in a system by taking variability in human behaviour (the primary underlying risk) into account. By selecting different technologies during the process, variability in technology is also considered.*

In a more recent study (2009) done by *Aven* [49], trends in quantitative risk assessments were researched. This study states that while techniques and methods introduced towards risk assessments processes are consistently increasing, the quality of the value added obtained from quantitative risk assessments is still questioned. The study by *Aven* provides the following recommendations:

1. The scientific basis of risk assessments needs to be strengthened;
2. A much broader risk description should be presented in risk assessments and more weight should be given to uncertainties;
3. Further research is required to improve modelling and analysis of human and organizational factors;
4. Modifications are required to implement the ALARP principle so as to incorporate the extended risk description, while risk tolerability levels should be used with care [49].

The points made by Aven directly support the research challenges of this study. The risk process presented in this research study must introduce modelling of operations to strengthen the engineering-scientific basis. This, combined with a systems engineering approach should provide a broader risk description in the preliminary design phase of the system. Human and organizational factors will be included in the modelling of risk during operations as these differ between organizations.

The research of *Dr Nancy Leveson* is also considered as she has made specific contributions towards safety engineering and risk management domains. She states in her book, *Engineering a Safer World* [50] that although the world of engineering has experienced a technological revolution, the basic engineering techniques applied to safety and reliability engineering (FTA and FMEA) had changed far less. *Leveson* believes that these existing challenges should be addressed by a systems thinking and systems theory approach [49]. She further makes her point clear in the following text:

> "*Traditional methods and tools for risk analysis and management have not been terribly successful in the new types of high-tech systems with distributed human and automated decision-making we are attempting to build today. The traditional approaches, mostly based on viewing causality in terms of chains of events with relatively simple cause-effect links, are based on assumptions that do not fit these new types of systems: These approaches to safety engineering were created in the world of primarily mechanical systems and then adapted for electro-mechanical systems, none of which begin to approach the level of complexity, non-linear dynamic interactions, and technological innovation in today's socio-technical systems. At the same time, today's complex engineered systems have become increasingly essential to our lives. In addition to traditional infrastructures (such as water, electrical, and ground transportation systems), there are increasingly complex communication systems, information systems, air transportation systems, new product/process development systems, production systems, distribution systems, and others.*
>
> *The limitations of the traditional models and approaches to managing and assessing risk in these systems make it difficult to include all factors contributing to risk, including human performance and organizational, management and social factors; to incorporate human error and complex decision-making; and to capture the non- linear dynamics of interactions among components, including the adaptation of social and technical structures over time*." From [49]

Leveson introduced a system-theoretic accident model (STAMP) which is further discussed in Section 4.5.5, in an effort to address these challenges.

The challenges identified by Leveson support the research challenges identified for this research. This research study will employ a systems engineering focus, used with operational modelling, to address the research challenges. The models presented by Leveson focus on operational accidents analyses in order to prevent similar future accidents, while the approach of this study will present a proactive analysis approach by means of operations modelling.

4.5 Human error and operational modelling

Human error is evident in any operational system – this is a well-known fact [50] [51] [52] [53]. Therefore, human error must be taken into account with the acquisition of new technology in South African mines. In this research, human error has two aspects, namely (i) human error introduced during system development, and (ii) human error introduced when operating a system. Both these aspects are addressed in this research since the focus is to introduce a structured risk management approach in the development phase, that is, when safety technology is introduced (as discussed in detail in the problem analysis in Chapter 3). The second aspect is addressed in the modelling of future operations and its associated risk.

A significant amount of research has been done on human error as the presence of human error is non-debatable. Also, due to the volatility and uniqueness of humans, this situation will persist – if not in operations, then in system development. Research done on human error is presented to assess current concepts, views and techniques available to assist the model development in this research, as discussed in the sections that follow.

4.5.1 The human error paradigm

Sydney Dekker is known in the field of human safety and reliability, specifically in the aerospace domain. Dekker presents two different views of human error which are the “old” (classical) view and the “new” (modern or systems) view, as shown in Table 5 on the following page.

It is clear that in the old / classical view, as presented by *Dekker*, the focus of responsibility shifts towards the human and human error, while in the new / systems view, error emanates from the system (in the true sense – a system with its core and all support elements). Thus, for the modern view, if a human error occurs, the possibility of such an error (control) should have been taken into account in the system design, that is, during development. Therefore, the system itself is to blame and not necessarily the operator. For example, when incompetent operators were appointed, the system is responsible as it should have foreseen such an event, and so on.

In the modern paradigm, *Dekker* states that employees do not come to work to do a bad or unsafe job. Employees are inherently “good” and often try to resolve multiple goals in a complex, dynamic environment. Although it often looks like a human error, one should realize that human performance could go wrong due to various factors

including cognitive fixation, plan continuation, stress, fatigue, buggy or inert knowledge (training), new technology, unexpected behaviour due to computerization and automation, and procedural adaptions, to list a few [51] [54] [55].

Table 5: Two views of human error [51] [54]

	Old (Classical) view	**New (Modern) view**
1	Human error is a cause	Human error is a symptom of a problem in the system
2	To explain failure, you must find errors, violations, incompetence, and mistakes.	To explain failure, do not try to find where people went wrong.
3	You must identify a worker's inaccurate assessments, wrong decisions, and bad judgments.	Find how worker's assessments and actions made sense at the time, given the circumstances that surrounded them.
4	Complex systems are basically unsafe.	Complex systems are not basically safe.
5	Unreliable workers undermine defences, rules and regulations.	Complex systems are trade-offs between multiple irreconcilable goals (safety and productivity).
6	To make a system safer, restrict the human contributions (automatic systems, tight procedures, strict supervision).	People have to create safety through practice at all levels of the organizations (a safety culture needs to be developed).

Both classical and new views are important in the mining environment in a balanced way. When production goals are pursued, it is inevitable that operators will bypass a system that limits production and safety goals will not be reached, and vice versa. Therefore, by balancing the old and new views, a portion of responsibility will lie with the system designers in that human limitations will be considered in the system design during acquisition. Similarly, a certain amount of responsibility will lie with operators to follow procedures as set out to achieve both production and safety goals during operations. Full apportionment of blame to management (including the engineering function) implies that humans will always follow procedures and will always make correct decisions under ideal conditions. However, in an agile environment such as the South African mines, this is not achievable and operators will show variability in performance that must be considered in an operational model.

4.5.2 Human error modelling methods and techniques

A significant amount of literature exists for human error analysis and modelling. Most analysis / methods are performed in the design phase of the system to assist with a design for human error. It is beyond the scope of this research to develop a specific model for human behaviour, but it is imperative to use literature to enrich the modelling of operations that involve technology, human behaviour, and error.

Techniques for human error analysis as found from literature are listed below:

- Task analysis [56] [57];
- Task analysis for error identification (TAFEI) [56];
- Checklist for identifying relevant human failure modes [57];
- Predictive human error analysis (PHEA) [56];
- Human failure modes and effects analysis (HFMEA); [57]
- Quantified human reliability assessment [56];
- Man-machine system analysis [53] [58];
- Improved job satisfaction [53] [58];
- Quantified human reliability assessment (HRA) [56];
- Probabilistic risk assessment (PRA) [53] [58];
- Technique for human error rate prediction (THERP) [53] [58] [59] [60];
- Empirical technique to estimate operator errors (TESEO) [53] [58];
- The probability tree method [53] [58];
- Pontecorvo's method of predicting human reliability [53] [58];
- Rooks model of human error occurrence [53] [58];
- Strategies aimed at changing the environment [53] [58];
- Influence diagrams and model of accident causation using hierarchical influence network [56];
- Human factors investigation tool (HFIT) for accident analysis [56];
- Organisational strategies aimed at changing organizational processes and the environment [53] [58];
- Time reliability correlation system (TRC) [59];
- SPAR-H Human reliability analysis method [61];
- Human event repository and analysis [52];

- Integrated dynamic decision analysis (IDDA) [62];
- Functional resonance accident model (FRAM) [63];
- Sequentially timed events plotting (STEP) [63].

The above techniques (or combinations of these techniques) can be used to develop a risk score and a systems-based framework for humans in operations. This is discussed in the following sections.

4.5.3 Human error and safety modelling applicable to this study

As is evident, a wealth of literature exists on human error, failure, and safety in socio-technical systems. As far as human error and failure are concerned, research is mainly focused on human activity at task level, where human-machine interfaces and interactions are analysed and modelled.

Human error is also analysed in accident analysis, which is a retrospective, systems-based approach to preventing future failures, not directly aligned with this research, but accident analysis adds significant value when an incident has occurred that must be analysed.

Most relevant research is done by *Dekker* [54] [55] *Demichela* [62], *Layman* [64], and *Embrey* [65]. Safety modelling has recently become more systems focused, with research from *Leveson* [66] at the cutting edge.

In a local (SA) study done by *Badenhorst* and *Van Tonder* in 2004 on operators of Eskom's Power Generating Group [53], the aim was to determine factors that lead to human errors. The results from this study showed that factors leading to human errors can be reduced (by as much as 70%), but that the responsibility of implementation lies with management [53].

This above finding on human error shows that the work done in this research is critical to support management in making proactive, informed decisions in the acquisition phase of socio-technical systems.

4.5.4 FRAM and STEP accident modelling

Both functional resonance accident modelling (FRAM) and sequentially time events plotting (STEP) model accidents retrospectively [63]. Retrospectively, however, it is easier to find root causes for accidents because an accident becomes deterministic after the fact and the history determines the flow of events. Nonetheless, STEP uses sequential event mapping (as a timed workflow) to describe the sequence of events that led to an accident. FRAM uses process blocks (functions) with

interdependencies to identify functions that “resonated” and consequently resulted in an accident. FRAM allows non-linear dependencies, performance conditions, and variability, all which provides a better understanding of how and why accidents occurred. Both methods contain inherent characteristics that can be applied to modelling before accidents occur.

A timed workflow, where tasks are executed in sequence, is normal to workflow modelling in systems engineering and can be applied to model repetitive tasks (that is, daily tasks executed in a shift). Process blocks that make up a complex, non-linear system can be used to model interdependencies in an abstracted space where system states can be modelled accurately. Each task will have a function, inputs, outputs, preconditions, resources, a time dependency, and controls (implicitly built into the overall state model). The use of process blocks / functions allows non-linear dependencies to be modelled. These principles will be applied in an operational model to proactively model system behaviour (including human behaviour) in this research.

4.5.5 The STAMP model

STAMP is a qualitative and comprehensive accident causation model developed by *Leveson* [66]. The STAMP model is specifically relevant to this study as similar design challenges to the challenges for this research were identified in the development of the STAMP model. The approach of this model is to address inadequate safety constraints found in design, development and operational phases of a system. In the STAMP accident model, safety is treated as a control problem, in order to handle complex, indirect, and nonlinear interactions of systems. Although the STAMP model uses traditional failure-based principles and methods as a basis, causal factors are also included in the model, namely dysfunctional interactions among non-failing components; software and logic design errors; errors in complex human decision making; organizational characteristics; and managerial, social and cultural factors [66]. STAMP is not only focused on analysis at component level, but contributes to each level of the organization, providing a holistic view.

More information and case studies relating to the STAMP process can be found in [38],[50],[67],[66] and [68].

The STAMP model supports this research since the approach is based on systems theory principles with human decision / action modelling. The research done in this study employs dynamic modelling of humans in operations – that is, everywhere humans have to decide and act, possible decisions and actions are modelled and simulated.

4.5.6 Human factor analysis

In a recent (2013) study done by *Demichela et al* [62] a method was proposed to qualitatively and quantitatively account for human factors. The approach uses the safety integrity level (SIL) of machinery that interface with operators. The research showed that it is critically important to include human interaction in a logical model when, together with quantification of human errors, models are drawn up for man-machine risk analysis.

The work of *Demichela et al* defines an improved method and framework for the integration of human and organisational factors into safety analysis by adopting an integrated dynamic decision analysis (IDDA) method, integrated into task analysis. This tool allows for the modelling of the logic of a complex system. It further allows modelling of all possible alternative states into which the system could evolve [62].

The focus of the research done by *Demichela* is on human safety at task level where electro-mechanical machines can physically harm individuals (this is also where the SIL rating is used). This type of analysis is an important part of physical interface design in the detailed product design phase, but is less focused on preliminary design where abstractions are used to model system states.

The research [62] *supports the principle of a human-centric, integrated approach to risk modelling. Human interaction must thus be included in a model, with quantification of human error. However, in essence a higher-level technique will be used as the focus is on operational modelling and acquisition.*

4.5.7 Process risk indicator (PRI) methodology

Layman et al [64] presents a methodology to determine emergent system properties (such as safety or reliability) in the early life cycle phases. A fundamental assumption of systems engineering is that risk mitigation processes should reduce system risks, but it may be that mitigation processes increase risk since these processes may not be appropriate for achieving a desired emergent property, or processes may not be followed correctly. The process risk indicator (PRI) methodology is used to analyse development of process artefacts in terms of safety and reliability. This analysis is done to quantify process risk that may lead to higher system risks [64].

In the risk modelling approach followed in this research, a risk modelling method must be ensured that identifies mitigation processes that could increase risk. This is why safety technology must be evaluated when integrated with normal operations. A relativistic approach should be followed to compare different technologies and associated processes in order to identify mitigation processes that may add risk.

4.5.8 Identification and prevention of human error

Embrey [65], a specialist in human factors, proposed a set of techniques and computer-based tools for prediction and prevention of human errors in gas plant operations, with a focus on risk management in process safety.

In his research, a software package is presented called the human factors workbench (HFW), comprising three integrated software tools. These tools support analysis of a task structure and prediction of errors and their consequences at human task or sub-task levels. A risk profile based on human factors can be developed that includes the probability of errors and the most cost effective human error mitigation, effectively implementing a risk score card for individuals. This software provides an estimate of the likelihood of errors with a simplistic graphical analysis toolset for visualisation of risk. This allows a designer to perform retrospective analysis of accident event sequences [65].

This approach to modelling and human error is significant to this research as a supporting tool to analyse human error at task level. By assigning risk scores to operators, it is possible to model operator decisions and actions based on these scores. Such an approach makes it possible to model behaviour at a higher level in the preliminary design phase before detail interface design is done.

To address human error in this research, a risk score approach is followed. Each operator or human interfacing with the system is scored according to a defined level of risk. Five different risk levels are used, where risk level 1 is associated with a worker that presents the lowest risk, while the highest risk score will be risk level 5. Worker risk levels must be determined by the human resources (HR) department of the organization and can be based on the human performance factors as identified by *Dekker* [54]. This risk score for each worker must be determined by psychometric assessments, work experience, training levels, culture, etc.

The definition of specific criteria for risk scoring of workers falls beyond the scope of this research, but risk profiles are used in this research to link human error to technology acquisition for safety equipment.

The use of a risk score allows one to determine the sensitivity of a system's performance with respect to human variability. In doing this, one can find a balance between investing in safety technology or investment in humans. For example, training and control cost can be reduced by appointing less risky operators.

This concept is further discussed in Section 5.3.5 and Section 6.5.3.

4.5.9 Risk analysis resources

Risk analysis and modelling require a level of knowledge, skill, and experience that may prevent a mine from performing risk modelling. *Sklet* [69] provides a list of accident modelling methods and the level of expertise required to execute an accident analysis (risk management is not accident analysis as such, but similar as it employs similar methods and techniques). The resulting finding shows that, in most cases, an expert or specialist is required to perform a reliable risk analysis.

Observations made in the mining environment confirm that this level of skill is not always present, but that the task of risk analysis is critical and modelling must be done, regardless of the availability experts and specialists. Visualisation of risk in an understandable form is also necessary and will be addressed in the risk management model of this research.

4.5.10 Operational risk modelling tools

As the complexity of systems increased over time, specific modelling software packages were developed to assist with complex modelling and simulation of human, organisational and operational risk events.

The modelling technique (and software) required to support this research must be able to simulate operational events of real-world scenarios in socio-technical systems. When risk exposure is determined from such an operational model, given specific technology and differing levels of human performance, risk can be reduced by reducing the number of, or by adjustment of, high risk functions.

A number of discrete process modelling tools exist, with selected tools listed and described in Table 6 below:

Table 6: Available discrete event simulation software [70]

Simulation Tool	Features
AnyLogic	• Multimethod simulation modelling; • General purpose simulation; • Supports agent based, discrete event, and system dynamics methodologies.
Arena	• Business Process Simulation; • 2D and 3D animation.
Enterprise Dynamics	• Specific to the industries of Logistics, Airport, Transport, Warehouse, Pedestrian and Educational.

ExtendSim	• Agent based modelling; • Continuous and discrete rate modelling; • Statistical distribution fitting.
FlexSim	• Mainly focussed on manufacturing and logistical industries; • Object oriented approach.
GoldSim	• Probabilistic simulation software; • Combines system dynamics with discrete event simulation; • Monte Carlo simulation framework.
Lanner	• Process and experimentation modelling; • Graphical 2D and 3D interface; • Scripting Interface.
MS4 Modelling Environment	• Complex system modelling; • Discrete event simulation system model development via natural language or Java; • Compose complex systems via system entity structures;
Plant Simulation	• Focussed on production systems simulation and optimization.
ProModel	• Continuous process modelling; • Assist with evaluating, planning and design of manufacturing and logistic processes.
Renque	• General purpose discrete event simulation; • Integrated with Visual basic scripting; • Graphical interface for design and operation.
Simcad Pro	• Dynamic discrete and continuous simulation; • Visual interface; • No coding environment; • 2D and 3D animation.
SIMIO	• General purpose modelling; • Complex system modelling; • Object oriented; • Graphical design and process flow interface; • 2D and 3D animation.
Vanguard	• Human level simulation for vulnerability analysis; • Military based (force-on-force).

4.5.10.1 SIMIO

SIMIO is a simulation software tool that provides a unique way to simulate real world scenarios. This allows a designer to examine future operations and make informed decisions based on outcomes of simulations. SIMIO follows an object-orientated approach to allow a designer to model complex systems [71].

SIMIO is not specifically used as a risk management tool, but rather as a programming language that allows control of low-level functions which allows construction of complex operational models. Although SIMIO was selected for this research, traditional engineering software tools (for example, MATLAB, C++, and Java) could also have been used to generate similar results.

The advantage of using SIMIO is its ability to run simulations with a visualisation capability, while providing functional building blocks (process blocks) as the fundamental elements of the model.

Different simulation tools were evaluated and identified as viable tools for modelling processes in this research. The SIMIO simulation package was selected for operational modelling in this research for its availability, flexibility, support of complex modelling, and ease of use. Although other tools could have been used in this research, availability of SIMIO was the main consideration. An integrated operational model and simulation results of an actual safety system are presented in Chapter 6 of this document.

4.6 Systems engineering

Human modelling in socio-technical systems is difficult to do without an operational framework. Systems engineering (SE) provides such a framework as the first step of constructing a model that draws together all elements of a system, including behavioural and architectural aspects.

Systems engineering also provides a full life cycle view of operational systems, which allows the designer to analyse future operations before commencing with a design. This approach will be followed to address defined research challenges.

This section describes the fundamental definition of systems engineering, after which the life cycle phases are briefly reviewed for the sake of completeness. More specifically, the importance of systems engineering in reducing operational risk is highlighted and comments are provided on the importance of specific phases in the life-cycle.

4.6.1 Systems Engineering background and definition

The most important standards that define systems engineering include MIL-STD-499B (Military Standard) [72], EIA 632 (Electronic Industries Alliance) [73], ISO/IEC 15288:2008 (International Organization for Standardization and International Electrotechnical Commission) [74], IEEE 1220 (Institute Of Electrical and Electronic Engineers) [75], NASA SE handbook [76], and the INCOSE Handbook (International Council of Systems Engineering) [77]. Although the information of these sources correlates, the definition for systems engineering of INCOSE was used in this research. Further information and comparisons between the abovementioned standards is found in literature (*Sheard* and *Lake* [78]).

The definition of Systems Engineering, as quoted from the INCOSE Handbook is as follows:

> *"Systems engineering is a discipline that concentrates on the design and application of the whole (system) as distinct from the parts. It involves looking at a problem in its entirety, taking into account all the facets and all the variables and relating the social to the technical aspect.*
>
> *Systems engineering is an iterative process of top-down synthesis, development, and operation of a real-world system that satisfies, in a near optimal manner, the full range of requirements for the system (Eisner2).*
>
> *Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs" (INCOSE3)* [77].

This definition clearly defines systems engineering as a perspective, a process, and a profession that is interdisciplinary, iterative, socio-technical, and holistic. Systems thinking forms the basis of the systems engineering perspective, where in systems thinking the activities of discovery, learning, diagnosis, and dialog lead to sensing, modelling, and talking about the real world to form a better understanding of complex systems [77].

4.6.2 The systems engineering life cycle

A systems engineering life-cycle process begins by identification of a need and extends through requirements definition, functional analysis and allocation, design synthesis and evaluation, validation, operation and support, and disposal phases of a system [79]. These systems engineering phases are shown in Figure 16 and are discussed in the sections that follow.

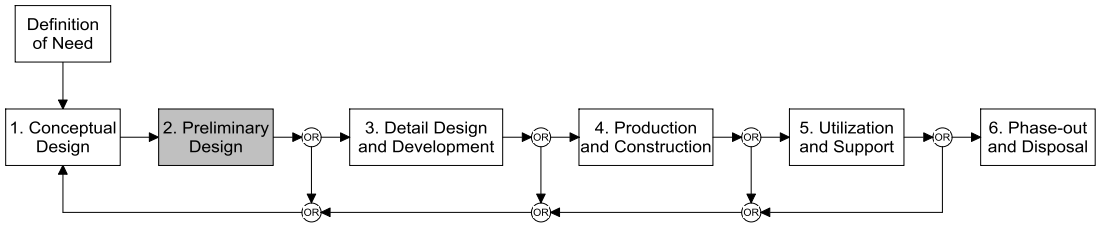


Figure 16: Systems engineering life cycle phases [79]

The preliminary design phase is highlighted in the figure above as the focus of this research falls on this phase. The remaining phases are equally important, but the preliminary design phase was identified as the phase where risk identification and modelling adds significant value at operational and technological levels.

4.6.2.1 Conceptual design

The conceptual design phase is initiated by the definition of a need as defined by the client. The need, in the mining environment, is typically for a mitigating technology to control an operational risk by addressing all safety aspects in the conceptual design phase. This early, high-level life-cycle activity has the purpose to establish, commit and predetermine the function, form, fit, cost, and development schedule of a desired system. Activities of importance to conceptual design include the definition of system operational requirements (mission and high-level functional capability, and non-functional requirements such as environmental, physical, legal, etc.), definition of a system maintenance concept and lower level functional requirements. Lower-level functional requirements follow from operational requirements, but are typically not analysed in detail in this phase, unless significant technical and / or project risk is evident. Advance project planning is done and includes technical planning and project planning, captured in a systems engineering management plan (SEMP) and a project management plan (PMP), respectively [79].

In the concept phase, specific focus is on determining high level requirements. In the mining industry, where safety equipment is acquired, this phase sets the concept for a proposed mitigating solution. Once the concept has been finalised, the system is further analysed in the preliminary design phase. Due to the iterative nature of a systems engineering process, the initial concept is often redefined or altered with feedback from downstream phases.

In the current mining environment, a conceptual design is typically performed by the mine's engineering department. Once a problem has been identified and possible solutions have been analysed, high level requirements (operational requirements) are determined and provided to contractors to develop / supply technology solutions accordingly. A risk analysis on new equipment is also done in this phase, but lacks operational detail required to fully understand underlying causes of risk. A basic HAZOP is typically done to identify harmful materials, explosion and fire risks, man-machine interface risks, and so on. Limited operational modelling (functional / behavioural) is done as this requires substantial expert input.

4.6.2.2 Preliminary Design

The purpose of the preliminary design phase is to demonstrate that a defined system concept will meet performance and design specifications, and also that the concept can be produced with existing or new methods (buy or make) within cost and schedule constraints.

The preliminary design phase is divided into sub-sections, each with specific focus areas. These sub-sections are shown in Figure 17 and explained in the following sections.

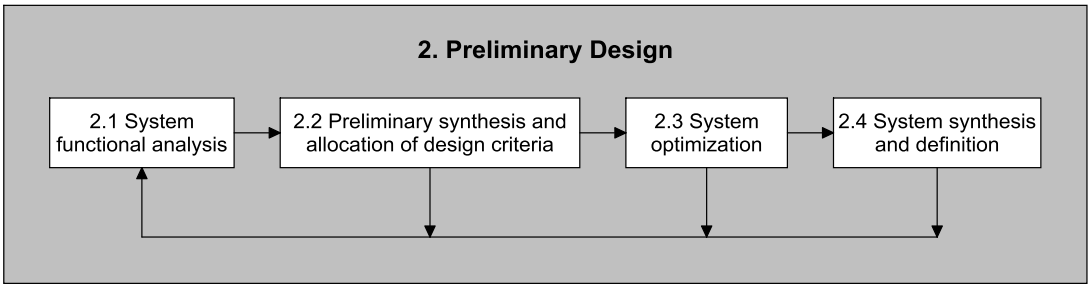


Figure 17: The preliminary design phase [79]

System functional analysis

Functional analysis is an integral part of systems engineering. This analysis draws together all system elements by providing important information for (i) the establishment of functional capability, (ii) identification and definition of maintenance functions, (iii) identification of test requirements, (iv) identification of critical functions and fault analysis, (v) identification of interfaces, and (vi) allocation of performance and design requirements. Results from the functional analysis allow for creation of support data in terms of assembly / manufacturing procedures, operator procedures, repair procedures, and further data evolving from functions and functional architectures. A functional analysis also provides an important framework for modelling of a system in an operational environment.

A particular advantage of a functional analysis is the identification and design of user functions (tasks) and interfaces. In practice, it is not uncommon for engineers to design equipment where a user is expected to adapt to the system, instead of the system being adapted to the user. When usability is included as a design requirement in the functional analysis, all functions executed by users can be identified while provision can be made in the design to simplify these functions and their associated interfaces.

The functional analysis is performed by executing the following steps, namely to define system operational functions, identify system maintenance functions, define system architecture, and to perform a system analysis (including identification of alternative functions and sub-functions) [79].

A functional analysis forms critical part of the method developed in this research. This allows a designer to implement real-world models from abstracted functional flows to determine all performance parameters, including risk / exposure factors, that are used to characterise a system. The system is analysed to find all critical functions that contribute to high risk. A technique to identify and manage high risk functions is developed as part of this research study as a specific contribution to the body of knowledge in the design science research framework. Alternative functions must be identified to replace or adapt high risk functions, or controls must be put in place. The overall system risk is thus reduced though an iterative process.

Preliminary synthesis and allocation of design criteria

Performance and design criteria must be linked to functions and functional units of the system architecture. Each function must have its own performance requirements, while design criteria are generally linked to functional (physical) units. Physical units

include a physical architecture consisting of assemblies, sub-assemblies, components and interfaces of a system. Important steps of allocation include the allocation of performance factors, design factors and effectiveness requirements, the allocation of resources to functions, the allocation of system support requirements, and system analysis and evaluation [79].

A resource allocation links system functions to identified resources. This allows the designer to perform a failure-mode analysis as each resource failure will have an effect on specific functions at different system and sub-system levels. A resource allocation is done by using a resource allocation table.

A resource allocation is used in this study to determine and allocate risks to resources. Functional flows and states for each resource are defined to allow a designer to build a simulation model for the operational level of the system. By allowing failures of resources in this model, risk can be determined in terms of hazardous exposure and production loss.

System optimization

Different architectures are considered as candidate solutions for a system's functional requirements in the design of a system. An abstraction is performed to provide a framework to be used in trade-off studies. An abstracted functional unit (as an element of an architecture) can be realized by using technologies and / or other resources. Selection of the best solution for a functional unit results in the optimization of that functional unit, given the overall system requirements.

Optimization, in this research, does not imply mathematical optimization where a goal function is explicitly defined and optimized using mathematical or heuristic algorithms, but rather optimization in an operational context. It is not sensible to change a system architecture without including a designer (or design team) and other human resources in the optimization feedback loop. A final system configuration is selected from a set of functions and configurations as provided by designers so that constraints (in the form of requirements) are met.

Important aspects of system optimization include system and sub-system trade-offs and evaluation of alternatives [79].

A trade-off (as a rudimentary form of optimization) forms part of the proposed method developed in this research. For this research, all trade-offs will have a "functional" focus to allow a designer to determine optimal functions of a system, given operational and human resource constraints.

System synthesis and definition

A system definition, captured in a high-level specification, is seldom complete at the onset of development. This implies that lower-level requirements must be developed by first developing an experimental evaluation model, which could be a simulation model or a physical model. This model enables a designer to evaluate system performance before operations commence. System synthesis and definition includes a preliminary design that includes performance, configuration, and arrangement / architecture of a system and drafting of detail development specifications [79].

A preliminary design phase provides a more in-depth analysis of a system to determine its exact configuration in terms of functions and interfaces.

The preliminary design phase is often neglected in the development process. This was observed during the development of electronic safety equipment for mines. The focus is thus on methods and techniques in the preliminary design phase as risk analysis in this phase provides sufficient depth to understand all contributing risk factors.

4.6.2.3 Detail design and development

In the detail design and development phase, lower levels of the system hierarchy are addressed. This includes activities that define sub-systems, units, assemblies, lower-level components, software modules, people, facilities, and elements of maintenance and support. In this phase, remaining detail requirements and design data for all system elements are derived and addressed, while selected components are procured / developed and integrated.

The focus areas of detail design and development are presented in Figure 18, and explained in following sub-sections.

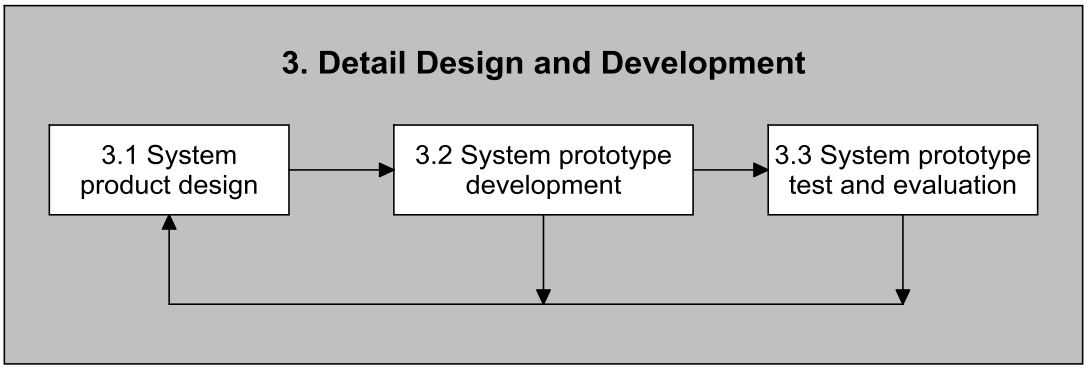


Figure 18: The detail design and development phase [79]

System product design

Activities performed in the system product design include detail design of software / firmware and electrical / electronic hardware, detail design of system maintenance and logistic support elements as identified in the high level functional analysis, and design of support functions provided by manufacturers of technology or software / firmware development tools. Also, design data and documentation such as documented case studies, design notes and statistical data, and software / firmware support tools should be generated. The system is analysed and evaluated, including test analyses and evaluation of test results. Finally, a design review must consider successes and possible adjustments, often resulting in adaption of higher level specifications.

The link between a concept and an actual product design is critical when risk is analysed. In the mining environment, as was observed, this link is sometimes absent, which leads to a discontinuity in product design. This is a technical risk that can only be addressed by employing a comprehensive preliminary design.

System prototype development

A prototype development phase consists of sub-phases where a series of prototypes is developed, resulting in a final prototype. Activities include development of interim development models, development of a final system prototype model, and development of system maintenance and logistic support requirements [79].

As part of the acquisition process in mines, prototypes are developed mostly by contractors. When a preliminary design is absent, the number of prototypes increases, and so do development cost and time. The result is an increase in project and operational risk as mining operations continues without safety equipment. Developmental prototypes should not be used in actual operations as human lives are at risk – a situation that can occur in mines if the contractor is not fully managed. For this reason, it is critical to perform proper operational risk modelling in the preliminary design phase.

System prototype test and evaluation

The system test and evaluation phase is characterized by testing of the prototype system and equipment, test data analysis and evaluation, test reporting, system analysis and evaluation, and modifications for corrective action [79].

Detail design and development is iterative in the systems engineering process. Once this phase has been completed and the final development model meets all

requirements as determined in the preliminary design phase, production and construction are done.

Although the primary contribution to this research is made in the preliminary design phase – where system risk is determined – detail design and development were also done as part of this research. Three physical models were developed, built and implemented – this was done as part of validation for this research.

4.6.2.4 Production and construction

The following activities are performed in the production and construction phase, namely production and construction of system components, acceptance testing, system distribution and operation, system assessment, analysis and evaluation, and modification for corrective actions and / or product improvement [79] [80].

Acceptance testing is made difficult in this phase without acceptance criteria from the preliminary design phase. Risk-based modelling of operations in the preliminary design phase highlights critical operational functions that must be tested for acceptance – this will not happen unless a complete functional analysis and requirement allocation were done. This is an example of an upstream activity (or lack thereof) that affects downstream risk.

4.6.2.5 Utilization and support

Utilization and support activities include system operation in the user environment, system assessment, analysis and evaluation, and modifications for corrective action or for product improvement [79] [80].

The three candidate systems developed in this research were implemented in controlled operational environments. The feedback from these solutions was importance for the validation of this research.

4.6.2.6 Phase-out and disposal

The efficacy of a system is evaluated on a continuous basis to determine when a product has reached its maximum effective lifetime. Further considerations include re-evaluation of the relevance of an operational need, evaluation of effectiveness of the system performance given new operational requirements, a feasibility study of system phase-out versus system maintenance, and availability of alternative systems [79] [80].

Proper operational modelling is an abstract process using real-world operational parameters. This allows a system model to be reused and resources to be re-allocated in an upgrade. With the upgrade of a system without a model, a risk analysis is most likely repeated with limited use of prior knowledge. By using a validated system model, prior knowledge from the body of knowledge is incorporated into a new / improved model, underlining the importance of risk modelling in the preliminary design phase.

4.6.3 Implementing systems engineering

It is observed by *Blanchard and Fabrycky* that most of the problems identified in system development is due to a bottom-up approach to design, instead of using a disciplined top down systems engineering approach. Issues resulting from a bottom-up approach are a lack of overall requirements and often an approach of “deliver it now and fix it later” is followed [79]. This concept is illustrated in Figure 19 (on the next page) where a life cycle is shown on the horizontal axis, while the cost incurred, system specific knowledge, and ease of change is represented in terms of a percentage to the complete project. From this illustration it is evident that more information becomes available at later stages in the project, but is it more difficult to change the system (or requirements) and a large percentage of cost will have been incurred.

The illustration from Figure 19 shows the importance of the implementation of the systems engineering process as part of the acquisition process for mines. This indicates the importance of defining system risks in the operational domain in the early stages of an acquisition as it is easier and less costly to change system requirements and the concept at this early stage of the design. The focus of a risk-based acquisition process must be to find as much as possible information available (system specific knowledge) in the preliminary design phase to reduce the number of iterations in later stages of the life cycle.

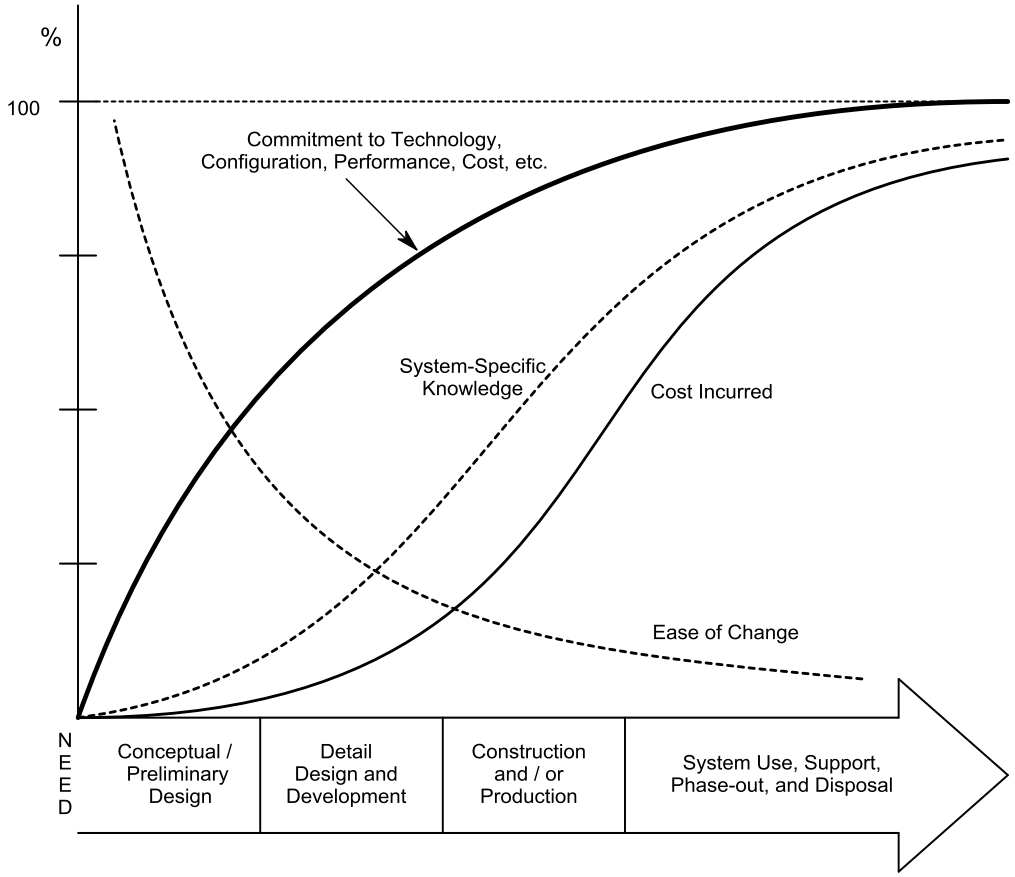


Figure 19: Life-cycle commitment, system specific knowledge, and cost representation [79]

The importance of the correct application of the SE process is underlined by *J.N. Martin*, where seven different candidate systems were identified to address a particular need. These candidate systems include an original “intervention system” with the aim to solve the real world problem. The intervention system is then placed in a “context system” and must be developed and deployed using the “realization system”. Thereafter, the intervention system, when installed in the context becomes the “deployed system”. This deployed system often introduces additional problems in the operational domain [81]. These operational problems need to be identified as early as possible within the SE life cycle.

This shows that development of “correct” technology is of critical importance. The challenge of knowing that the “correct’ technology was indeed developed must also be addressed – this can only be done by gaining a deep understanding of future operations in the acquisition phase by means of modelling.

4.7 Conclusion

The literature study presented in this chapter covered literature focus areas relevant to research challenges defined in Chapter 3. The process that was followed in this chapter was to research literature from different industries and engineering disciplines to determine possible solutions to the defined research challenges.

It was instructive to find validation of the research problem from literature in specialty fields – these served to validate the research problem and derived research challenges.

In summary, literature focus areas of this research are shown in the columns of Table 7 (on the following page) with the research challenges, as defined in Chapter 3, shown in the rows. This table is used to link a research focus area to each research challenge, where the information from a literature focus area is applied to address specific research problems as indicated in the table. Research problems are then translated to research solutions by using the information from the focus area. Research solutions are shown in the bottom row of Table 7.

More specifically, the focus of most literature on human error is on detailed modelling of human error at task level. This type of modelling is critically important, but does not provide an integrated view of technology in the agile mining operations in South Africa.

Thus, even though each separate research challenge can be addressed by an identified solution, an integrated solution was not fully dealt with in literature. A gap still remains between the acquisition and operational phases. Thus, the optimization of a system in terms of the functional requirements, given the human profile composition of an organization, is still lacking. A specific method will be developed and introduced during the following chapter to address this shortfall.

Table 7: Literature study focus areas applicable to the research challenges

Research challenges / **Literature focus areas**	Detail requirements are not defined	Sub-optimal safety technology often implemented	Focus is on hazardous exposure	Lack of integration and limited full life cycle perspective	The focus of risk assessments is mainly expert input and hazard based	Reactive incident risk management approach is followed	Impact of specific technology is not measured using a common norm	Lack of Human integration in risk assessment
Risk definition and terminology				↑	↑		↑	
The risk management framework		↑	↑	↑ ↓		↑	↑	↑
Risk analysis methodologies and characterization	↑	↑		↑	↑	↑	↑	↑
Existing risk assessment tools and techniques	↑	↑ ↓	↑ ↓	↑ ↓	↑	↓ ↑	↑	↑ ↓
Human error and operational modelling					↓	↓	↓	↑ ↓
Systems engineering	↑ ↓	↑	↑	↑ ↓	↓	↓		↓
Literature focus areas / **Research solutions**	Define detail system requirements in preliminary design	Follow an integrated approach	Follow a balanced approach(production, technology, safety, usability)	Follow an integrated SE approach	Use functional analysis during preliminary design to obtain all relevant information	Follow a proactive risk management approach	Follow a relativistic approach when comparing technologies	Introduce resource risk ratings to determine the operational effectiveness

Legend: ↑ ***- Literature focus area validates the research challenge***

↓ ***- Literature focus area contributes to the research solution***

Chapter 5
A risk based approach to electronic safety equipment acquisition

5.1 Introduction

Solutions to the research challenges have been identified and extracted from available literature in the previous chapter (kindly refer to Table 7). As discussed, a discontinuity still exists between acquisition and operations (engineering and mining). This life-cycle discontinuity should be addressed in the preliminary design phase, more specifically by addressing the following research solutions:

- Find the set of functions (including a functional architecture / configuration) that results in an acceptably low risk by removing / adjusting individual functions – this requires an integrated / systems engineering approach with a functional analysis;
- Determine the sensitivity of different system configurations (i.e. different products) relative to human performance variability by using risk scores for humans – this requires an integrated / systems engineering approach with a balance between technology, safety, and usability;
- Find a balance between productivity and safety across different system configuration (product) options, that is, find a balanced, cost-effective solution in a relativistic sense.

The above research solutions will be addressed in this chapter by the development of a risk-based model specific and relevant to the acquisition of electronic safety equipment on mines (with adjustment, but this approach could also be applied to other engineering fields).

5.2 The concept of activity-based risk (ABR)

The discontinuity above is addressed in this chapter by definition of an *activity-based risk (ABR)* model, which has been specifically developed in this research. The aim of this model is to integrate identified research solutions into a structured process, executed in steps, to perform a cost-effective system development in terms of risk and technology.

The activity-based risk process is executed in the preliminary design phase of the system life cycle. The ABR process and interaction with the SE process is illustrated in Figure 20.

The term, activity-based risk, is used in this research and will be the name for the method used to identify and treat high risk activities. This term "activity" is seldom used in literature in the risk context of this research – it is more often used in the context of risk related to physical human outdoor activities, sports and associated physical injuries. The definition of an "activity" in the activity-based risk sense is given below.

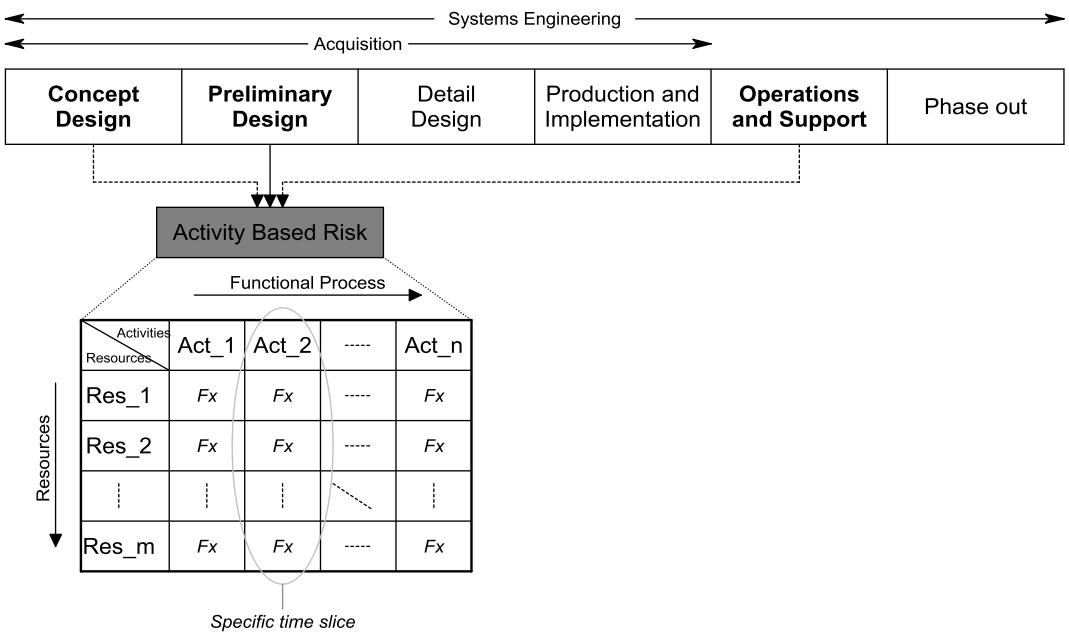


Figure 20: Activity-based risk within the SE process

The ABR method makes use of a systems engineering focus in the preliminary design, of which a functional analysis is an important element. In the ABR process, system activities are identified as subsets of a full function set. This is done to allow focused analysis of individual activities and identification of high-risk activities and

critical resources. Each system activity is a logical grouping of functions that draws together resources so that an integrated analysis can be done for individual activities. That is, smaller groupings of functions are analysed so that all participating resources are taken into account, as opposed to considering failures of individual resources.

Activity-based risk is a logical extension of the concept of baseline hazard identification as discussed in Chapter 4. Baseline hazard assessment defines relative risk of high-level activities (for example, stoping) in terms of its baseline risk profile, which in turn is based on environmental factors and activities conducted in such hazardous environments. High-level activities can be broken down into smaller activity groupings that combine tasks in a logical way. This classifies activity-based risk analysis – in this context – as a middle-out approach, as opposed to top-down or bottom-up approaches.

All system functions and resource states must be mapped to all system activities for modelling purposes. This illustration is shown in Figure 20, with resource functions and states represented by 'Fx'. Kindly note that 'Fx' represents more than one function / possible state of a resource, where functions / states may reoccur in the allocation. The ABR method allows a designer to determine risks related to failures of resources and system functions from the table. This analysis makes it possible to "optimise" a system in terms of functional requirements and to define desired characteristics of operators (or other human resources) that interact with the system.

ABR uses a simulation model (a SIMIO or similar type of operational simulation), based on the operational functions of a system and characteristics of system resources in order to deal with complexity issues. A simulation is done instead of a pure mathematical analysis as it gives the following advantages, namely:

(i) A grounded understanding of core operational activities (from a functional flow and architecture) is gained by engineering and operations / mining when drawing up an understandable operational model. The need for an understandable model is often communicated in regulatory documents as pure mathematical and statistical models require specialist knowledge and are difficult to fully understand;

(ii) Process blocks are defined from a functional analysis and used in simulations to implement complex functions, which assists with the understanding and modelling of a large number of resource functions, resources states, and interdependencies between resources and their states. This aligns well with the advantages of FRAM accident modelling, as discussed previously;

(iii) Integration of resources / an integrated view is preserved in the model as a system activity does not focus on a single resource (as is often done in human factor analysis), but on a set of integrated resources that take part in that system activity;

(iv) A relativistic comparison can be made between candidate systems / products because a simulation model is drawn up for each candidate system. Variations between candidate systems are implemented fairly easily as a basic simulation framework is constructed for the first model and then adapted for alternative models;

(v) Information is preserved in the model for future adaptation to a selected system. This prevents reinvention of solutions and provides a body of knowledge for business continuity.

Implementation of ABR is discussed stepwise in the following section, while the implementation of a real-world case study is discussed in detail in Chapter 6.

5.3 The process of applying activity-based risk

The ABR acquisition process model is illustrated in Figure 21 on the next page. This model is constructed by integrating solutions to the defined research challenges. This process and its associated procedures are discussed in detail in the sections that follow.

Note that the first two steps from the ABR process are performed in the conceptual design phase of the SE process, as indicated in Figure 20. The remaining steps are performed in the preliminary design phase.

5.3.1 Step 1: Define AS-IS design

With the focus on electronic safety equipment, the AS-IS design represents the current technology / safety equipment. In case no specific safety equipment exists and new technology is introduced, the AS-IS environment and operational functions must be defined by performing an operational analysis. This information will be used in the following steps of the ABR process when the system is compared to other candidate systems in a *relativistic* sense.

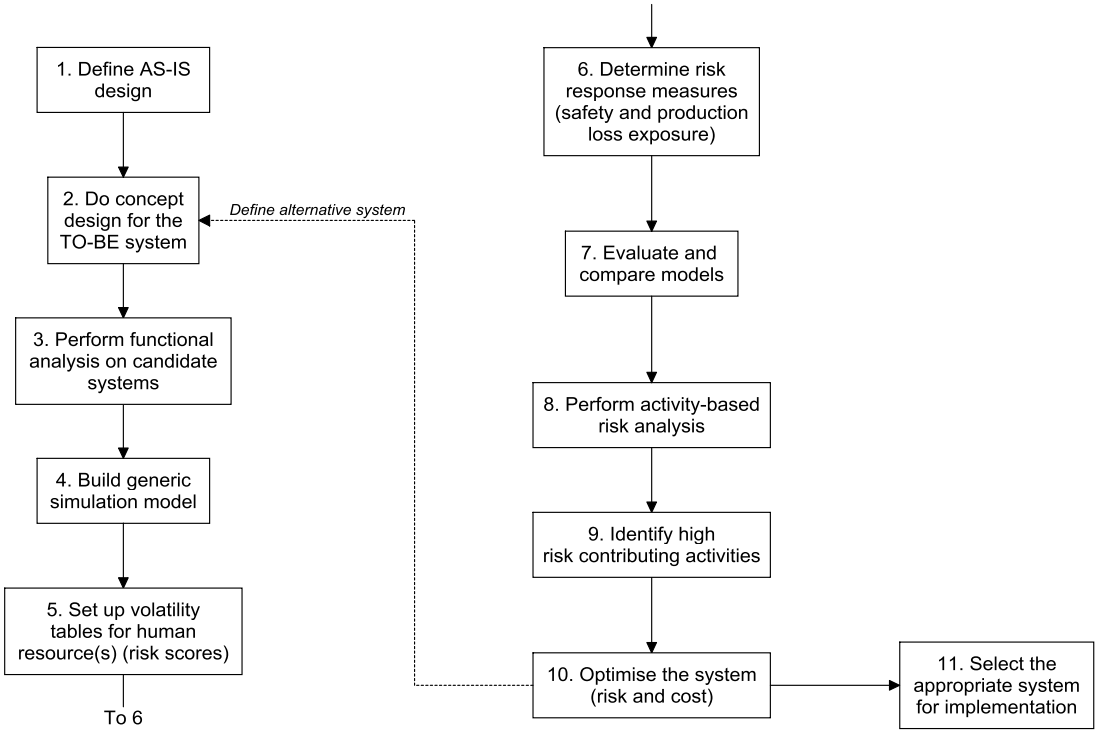


Figure 21: The ABR acquisition process

5.3.2 Step2: Do concept design for the TO-BE system

The conceptual design of a safety system is typically defined by the organisation. This defines the required characteristics for the TO-BE system.

From the conceptual design, operational requirements will be used as inputs to the preliminary design step, including an ABR method where a lower-level functional analysis is performed.

There is a feedback loop in Figure 21 that links back to the concept design. This allows a designer to improve the concept design iteratively with the goal of reducing losses and increasing safety. This is preferably done by using simulated systems as opposed to physically implementing candidate systems.

It is possible to define more than one concept to address an identified risk. It is imperative to consider more than one solution, or variations of a solution, as the focus of ABR is to follow a relativistic approach. All candidate models and solutions defined in the process are compared relativistically by using operational performance indicators related to risk (such as hazardous exposure time and production loss time, for example). Quite often, more than one candidate system is suggested in an engineering meeting, but an uninformed final decision is sometimes made. With an ABR acquisition process, candidate systems can be compared on a relativistic and equal basis.

5.3.3 Step 3: Perform functional analysis on candidate systems

The process of performing a functional analysis in the ABR acquisition process is shown in Figure 22 on the next page. These steps are important as it is the step where the most information is obtained from candidate system analysis. A functional analysis actually forces the designer (and all relevant stakeholders) to understand the operational and functional requirements of the system to its full extent, and "what if?" questions will be posed as the designer (and team) works through operational scenarios. At the end of this process, all uncertainties should be clarified.

The functional analysis performed in the preliminary design needs to be done for both the AS-IS and the TO-BE systems. If more than one candidate system has been identified, a functional analysis must to be performed on all candidate systems. At first this may seem excessive but commonly, if the designer (and team) starts with the functional analysis of a complex system, alternative concepts are usually altered versions of the initial system. Each step of the functional analysis is discussed in the following sections.

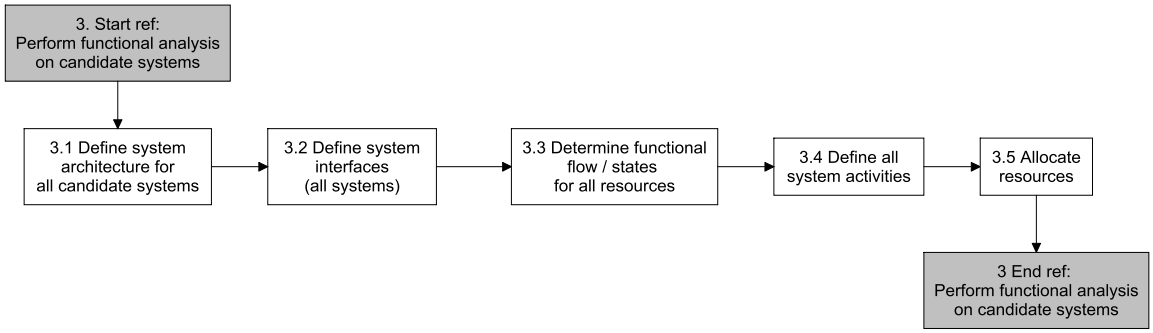


Figure 22: Functional analysis steps in the acquisition process

5.3.3.1 Step 3.1: Define system architecture for all candidate systems

An architecture is drawn up for each candidate system to define abstract static elements (functional units) of all conceptual models and their functional descriptions. All physical resources linked to functional units must be identified and be contained in the architecture. An example of a system architecture is presented in the case study in Chapter 6 for relevant AS-IS and TO-BE systems (Figure 25 and Figure 32).

5.3.3.2 Step 3.2: Define system interfaces

The system interface definitions form part of the system architecture and define all interdependencies between architectural components in both abstract and physical forms. Interfaces between resources (humans / equipment / environment) must be clearly indicated and defined. These interfaces must include:

- Functional interfaces in the abstracted model, showing interdependencies that will affect functional flow for modelling purposes; and
- Physical interfaces, such as mechanical, electrical, IT-related interfaces, and user / ergonomic interfaces.

An example of an interface diagram and definition is presented in the case study, Section 6.4, Figure 26 and Figure 34.

5.3.3.3 Step 3.3: Define functional flows / states for resources

All resource states and functions are defined, where resources typically include people (operators and other end-users of the system) and equipment (core operational equipment and safety system equipment) inside an environment.

For ABR, a functional flow is drawn up, augmented by event trees to account for human resource variability. The flow includes functions of human operators and other end users of the system. In an event tree, all possible routes are established by evaluating all possible decisions and actions taken by a human resource, given the operational flow and environment. A detailed example of these flows are contained in the case study in Section 6.4, Figure 27, Figure 28, Figure 35 and Figure 36.

Where human functions are modelled in an event tree, equipment and the environment are presented as states. This allows a designer to define system state diagrams of all candidate systems (electronic safety equipment) together with operational equipment and the environment that interface with the candidate system. Examples of state diagrams are shown in the case study, Section 6.4, Figure 29 to Figure 31 and Figure 37 to Figure 39.

Each function and state is numbered systematically for reference and traceability purposes.

The definition and clear documentation of functional flows and states are critical to the ABR process, as these will directly assist with implementation of a system model when the simulation model is constructed, as discussed in step 4 of the ABR process. State modelling requires specialist knowledge on the states that safety equipment can assume – safety equipment designers must thus be part of functional modelling.

5.3.3.4 Step 3.4: Define activities

System activities must be defined for all candidate systems. System activities are subsets of the overall function set and are logical activities of a system, for example, phases of a functional flow over time. Essentially, a system activity is a logical grouping that draws together all participating resources in a subset of the overall functional flow. Thus, a system activity is not a single resource (such as the case with human task analysis), but includes resources that function together to execute a specific activity (kindly refer to the resource allocation in step 3.5).

Note that activities must be common across candidate systems to allow for a relativistic comparison of ABR results. Thus, if an activity is identified in one candidate system, and the same activity exists in an alternative candidate system, this activity must be clearly defined in a functional flow for both systems.

With activities having been defined, it is critical to identify transitions between activities. Transitions between activities, such as is the case with interfaces, is where risk conditions usually change. For example, changing from a safe to an unsafe state must be coordinated between resources, and specific attention must be paid to transitional effects (also called transient effects).

A full set of activities can be defined by starting with the most complex candidate system. From there, activities can be removed or altered to define alternative candidate systems.

5.3.3.5 Step 3.5: Allocate resources

A resource allocation must be performed for system activities from the previous step. The resource allocation is performed in a tabular format with system activities along columns and resources along rows. Functions and states for each resource must be mapped to each activity using this table. All functions and states were determined in the ABR step 3.3. Resources must be presented as primary and secondary resources contributing to an activity. When an activity is executed by a specific human resource and equipment that human and equipment will act as primary resources while remaining resources do not have direct impact on this activity. The remaining resources are seen as secondary resources in this activity, but these resources will still be performing functions and must be in defined states. All possible states must still be mapped in the resource allocation to support modelling. An example of a resource allocation is shown in Section 6.4, Table 11 and Table 12 of the case study.

The output of the resource allocation is the first indicator of risk relating to resources in a system. This table allows identification of critical resources – i.e. resources that partake in many functions – and the impact on system activities when such a resource would fail. This allows a first step of risk mitigation by selecting alternative functions and resources. Although risks from this table give a first level of risk visibility, a more detailed risk analysis is performed in the following steps of the ABR acquisition process.

5.3.4 Step 4: Build generic simulation model

A simulation model must be implemented for each candidate system in the defined operational environment. Outputs from such simulations are used to identify risks in the later steps of the ABR acquisition process.

SIMIO software provides the advantage of implementing all candidate systems in terms of processes (process blocks). The functional analysis performed earlier in the ABR acquisition process clearly defines the processes for simulation, but resource states are also modelled and included in the SIMIO model – an advantage of using this simulation software as it supports multiple complex resources and states.

Functional flows (translated to event trees) that include human resource decisions and actions can be implemented as process flows in SIMIO, while states of equipment are used to program the model and drive interaction between resources according to the functional flow. This approach simplifies analysis of operationally complex models significantly.

An advantage of simulation software (particularly, SIMIO) is visual representation of system elements and their interactions when a model is executed. This is helpful during the development of a model as interactions can be visually verified. This visual representation also assists when communicating a model to stakeholders.

The selection and validation of operational performance parameters are important when constructing an operational model. Performance parameters define activities in functional flows and must be defined and allocated to represent real world scenarios accurately. System performance is dependent on risk profiles / scores of human resources in many instances. Volatility tables are generated to assist with parameter selection in such cases, as described in the following section.

A designer (or design team, rather) defines candidate system models with their parameters and operational performance measures so that parameters and performance measures agree and align across different models. This is done to allow a relativistic comparison between candidate models.

A degree of randomness must be allowed in human performance parameters. For these parameters, minimum, maximum and mean values are assigned to define a probability distribution function that describes variation in performance. The simulation tool must allow for such variations to support complex modelling of systems with a probabilistic nature, as is the case in safety models.

The detailed implementation of a simulation model in SIMIO is presented in the case study in Section 6.5.2.

5.3.5 Step 5: Set up volatility tables for human resources

In ABR, volatility tables are used to introduce human error in a multi-dimensional operational context. In order to draw up such tables, the designer has to define risk scores for human operators and other end users. It is possible to use psychometric modelling to draw up risk scores for operators ([51] [54] [65]) particularly those operators that work in high risk environments.

Therefore, in the development of risk scores (associated with risk profiles), human resources must be rated in terms of human factors as discussed in Section 4.5. This risk rating / level of a human resource is used in the simulation model to define parameters of a probability density distribution for failures at specific tasks in an operational workflow, as supported by SIMIO.

Volatility tables are thus set up for activities where humans deviate or fail. Decisions and / or alternative actions at branches in the event tree were identified in the functional analysis where all possible branches in the system's functional flow were defined.

The operational model thus combines humans and technology through operational workflows (functional flows), event trees, and resource allocations for each activity. This is done in a multi-dimensional operational environment, given all system resource states and interdependencies.

It is possible that parameters are not estimated accurately, but the relativistic approach followed in the ABR method largely alleviates this issue. Bear in mind that the ultimate aim of this work is to obtain the most appropriate safety technology by following the ABR acquisition process, which is relativistic / comparative in nature. That is, all candidate systems will make use of the same human resources with the same parameters when compared, which makes the selection of human performance parameters important, but not overly critical.

Development of specific risk profiles for humans does not fall inside the scope of this research, but literature verifies that risk scores / profiles have been successfully implemented in commercial software (Human Factors Workbench), as discussed in Section 4.5.8. For this research, a risk rating from 1 (low risk) to 5 (high risk) is used for human operators.

An example of the identification and implementation of deviation functions for a real world case study is represented in Section 6.5.3.

5.3.6 Step 6: Determine risk response measures / factors

Risk response measures must be identified in the simulation model to represent risk in an operational sense ("risk" in an operational environment has limited meaning as it is a broad term, and equivalent measures are used for ease of understanding, as observed during the case study). These measures can typically be time, number of failures, etc. Risk response measures are dependent on the type of risk being analysed and are selected to be semantically appropriate in an operational environment.

In the mining environment, two types of measures were identified for research on acquisition of electronic safety equipment. These measures relate directly to safety and production. Safety and production are juxtaposed and must be balanced in a production environment. Measures that align with safety and production risk are hazardous exposure (time) and production loss (time), respectively. This approach is also followed during the case study presented in Chapter 6, where the implementation of the response parameters is also discussed (Section 6.5.6.3).

Hazardous exposure is the time a human operator spends in a hazardous environment when the system is in an unsafe state. Production loss time is production time lost due to suspension of operations for safety and other reasons.

One may argue that hazardous exposure does not always lead to an accident, and that time lost for production does not imply production would have taken place. However, the probability of an injury or fatality occurring when the system is in an unsafe state is proportional to the time operators spend in hazardous environments, and production time lost could have been used for production in a productive organization. Moreover, a safety culture may increase or decrease the probability of injuries and fatalities, and a production culture affects the probability of production in a similar fashion. However, one has to bear in mind that the purpose of this research

is to perform a relativistic comparison between candidate systems as all measures will apply to all candidate systems.

Some activities will be more risky than others – this is the purpose of performing activity-based risk, namely to identify those activities in which hazardous exposure will be probable with severe impact. The probability of an accident will be less when a system is in an unsafe state which is communicated to workers. However, when a system state changes from a safe to unsafe condition and this status change is not communicated to workers, accidents are more likely, as will be seen from the case study.

5.3.7 Step 7: Evaluate and compare models

Multiple simulation runs must be executed on account of the stochastic nature of human activities in the process models. The number of simulation runs must be selected such that response measures provide results with an acceptable confidence interval, given a specific confidence level. In the case study presented in Chapter 6, 200 simulations were run for all scenarios. With this sample size, a maximum confidence interval of 6% of the range of response values was determined, given a confidence level of 95%. From the response measures, trends and worst case scenarios were determined, given the minimum and maximum values of these measures. The number of simulation runs depends on complexity of a model and taking into account the range and volatility of parameters.

Once the number of iterations has been set, and input parameters have been defined, simulation response measures can be evaluated for each system. The goal is to obtain the minimum hazardous exposure and minimum loss in production time.

Response measures of candidate systems (AS-IS and all candidate systems) can be compared to determine production loss and hazardous exposure for each system. The effects of different human resources (risk profile levels) on the system are also available for evaluation. Simulation results allow comparison of candidate systems in terms of quantified response measures.

In essence, different systems are compared by taking into consideration system sensitivity with respect to human variability in a predefined operational environment.

5.3.8 Step 8: Perform activity-based risk analysis

This step is imperative to the ABR acquisition process, as this is the point where risks associated with activities are identified. In this step, a table is constructed indicating

the impact when deviations or failures are introduced into a specific activity. This allows identification of high risk activities that are sensitive to human variation in the system (ABR Step 9). These activities can specifically be addressed in a design iteration when doing system optimisation (ABR Step10).

The process for Step 8 is shown in Figure 23, where these steps are discussed in further detail in the following paragraphs.

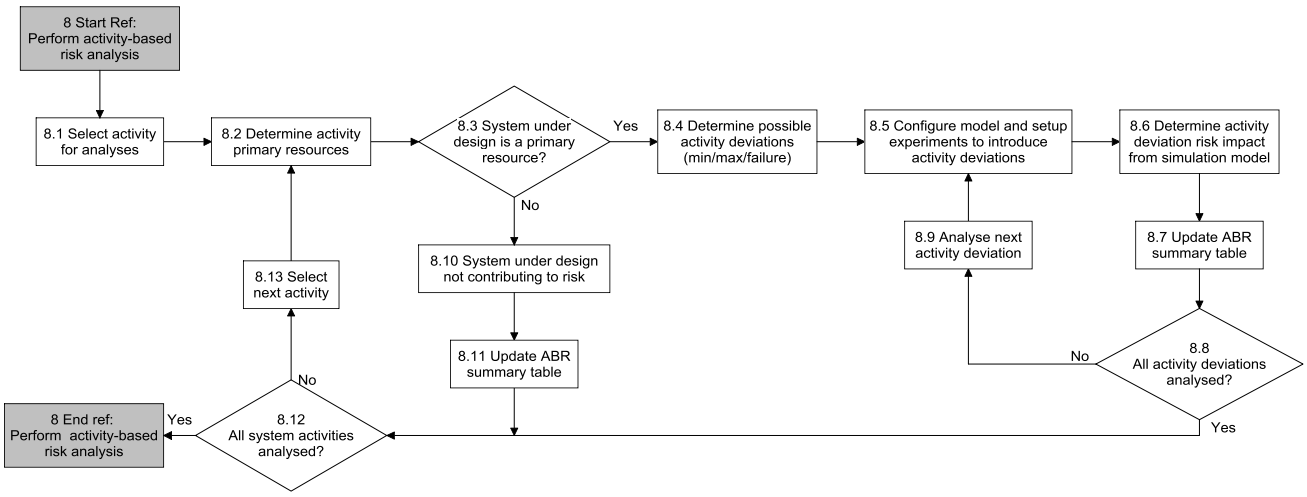


Figure 23: Step 8: Perform activity-based risk analysis

All activities identified in Step 3.4 are analysed in this ABR process. Activities are analysed sequentially (Step 8.1), after which primary resources for activities are verified (Step 8.2) – primary and secondary resources were identified in Step 3.5 when the resource allocation was done in the functional analysis. Identification of the resource relationship (primary or secondary) now becomes relevant to the ABR step as this determines whether or not an activity must be further analysed.

As discussed, a primary resource is a resource that performs a function in the system activity being analysed.

When a candidate system's technology (equipment) does not act as a primary resource for an activity being analysed (Step 8.3), the candidate system does not contribute to risk for this activity (Step 8.10). The ABR table is updated with this information showing that the system acts as a secondary resource for this activity (Step 8.11). The next activity is selected for analysis (step 8.13) until all activities have been analysed.

When the candidate system acts as a primary resource to an activity being analysed, it is necessary to determine all the possible human variations / deviations for this activity (Step 8.4). Typical deviations that can be introduced include extended time to execute a task and failure to execute a task. In many activities, a failure would result in the activity not being performed. Once possible deviations have been determined, each of these deviations is implemented and simulations are run for the complete system including all variations (Step 8.5). Response measures from this simulation are compared with response measures of the “normal” model, that is, the model without deviations. This comparison shows the impact of a deviation on an activity (Step 8.6). The impact must be updated in the ABR summary table (Step 8.7) after which the following deviation is analysed, simulated and evaluated (Step 8.9). This process is repeated for all possible deviations in each activity (Step 8.13). Once all activities have been analysed and the ABR table has been completed, high risk activities are identified for adaptation, replacement, or removal.

5.3.9 Step 9: Identify high risk contributing activities

High risk activities are summarised in the ABR table. This table indicates the impacts of deviations on different activities. Activities that are sensitive to deviations are identified as critical and are addressed in the optimisation step of the ABR acquisition process.

5.3.10 Step 10: Optimise the system

The system can be optimised for risk response measures by addressing high risk activities. This is achieved by evaluating candidate models where high risk activities are altered or where risk controls are added. Each candidate system is analysed using ABR and evaluated to determine the impacts on activities for all systems, until an “optimised” system has been reached.

The winning / successful system is further optimised for cost by adapting / removing high cost functions and / or activities. This is achieved by reducing functionality of the successful system. This must be done using results from ABR to ensure inclusion of critical features and exclusion of redundant features. With every change, the complete system must be re-evaluated.

System optimization for cost and risk in the acquisition process is illustrated in Figure 24 and is further detailed in the paragraphs that follow.

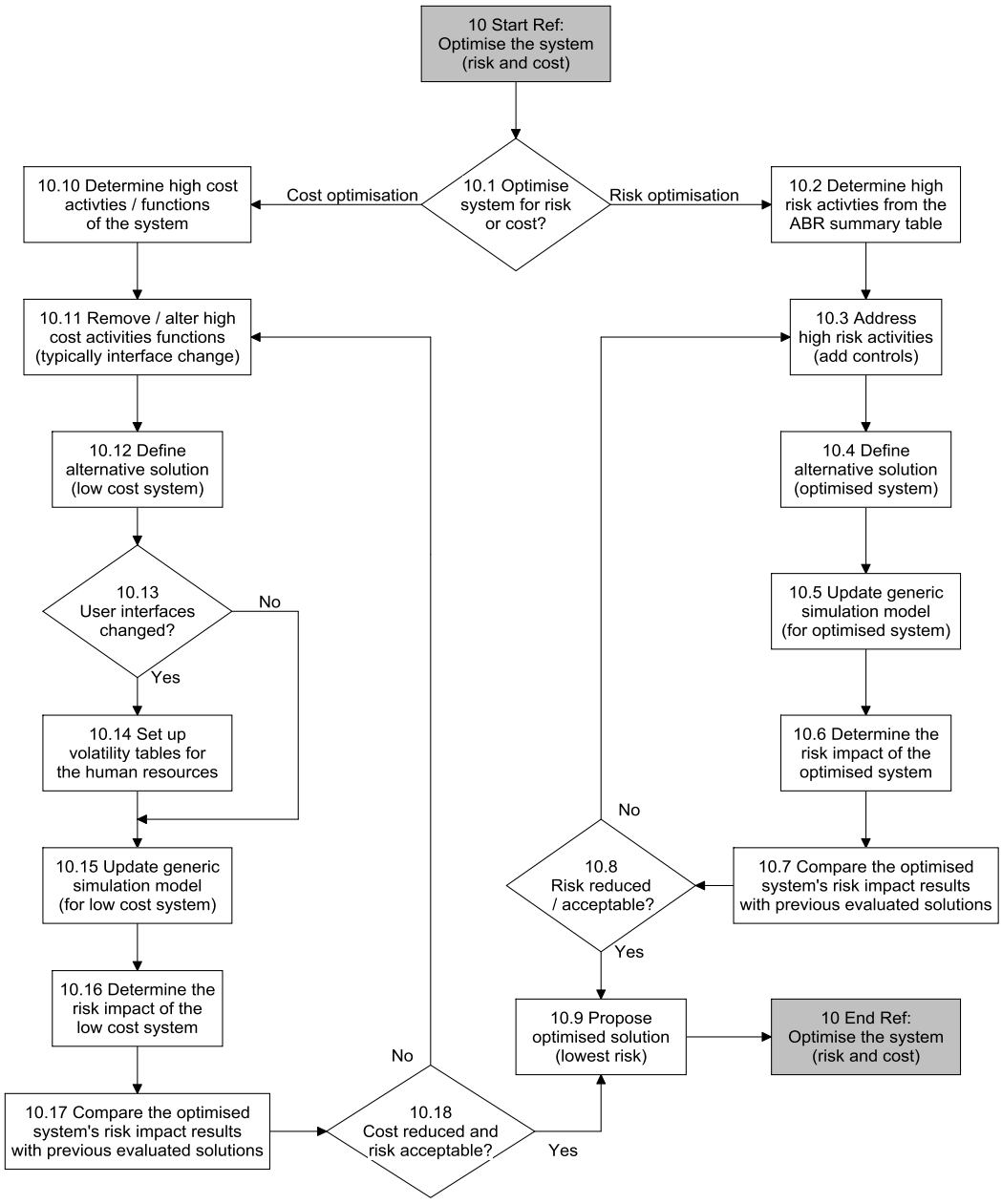


Figure 24: Step 10: Optimise the system

When the system is being optimised the process starts with risk reduction, after which cost reduction can be done as the high risk activities that must be included in the final solution have been identified (Step10.1). To optimise for risk, high risk activities are identified from the ABR summary table (Step 10.2). A new candidate solution is defined (Step 10.4) by adjusting or removing sensitive / high risk activities (Step 10.3). The simulation model must be updated to represent the new candidate system model (Step 10.5), after which response measures can be determined (Step 10.6). This allows determination of impact of a new candidate system and results to be compared with results from previous results (Step 10.7). If high risk activities were

addressed appropriately, this new system should show reduced risk, especially for the scenarios where more risky resources interact with the system. If risk has not been reduced (Step 10.8), further mitigations can be defined. When risks have been reduced to an acceptable level, the winning technology (product and system) is proposed for further development and implementation (Step 10.9).

Once the system has been optimised for risk, the system is optimised for cost. In this phase, high cost activities and functions are determined (Step 10.10). These functions are altered or removed (Step 10.11) to define an alternative candidate solution (Step 10.12). If an altered system impacts on human-machine interfaces (Step 10.13), new volatility tables must be set up (Step 10.14). The simulation model is updated to the alternative candidate model 10.15), after which response measures are determined from simulation (Step 10.16). New response measures are compared against measures of the initial system (Step 10.17). When optimising for cost, risk may increase from removal of safety functions, product features, and interfaces. This has to be considered in the broader context of the organization to take into account the organization's appetite for risk.

This optimisation cycle in the ABR method allows for risk reduction by adjusting and / or removing high-risk functions, but also provides valuable information on the sensitivity of the system with respect to human performance variation. With this information, a system can be optimised up to a point by altering technology, after which residual risk must be reduced by addressing human factors specifically. Notably, changing human factors is done by changing organizational policy and culture, which results in change of support processes (training, safety awareness, etc.), and operational measurement and control processes and procedures.

When optimising a system for cost, the designer and other stakeholders can determine a point where it is more cost effective to use a limited (more affordable) system with reduced functionality, and address residual risk at HR level, instead of investing in further technology. The acquisition method with ABR will show where the point of diminishing returns lies.

An example of this optimisation process (risk and cost) is illustrated in the case study presented in Chapter 6 (Section 6.5.9).

5.3.11 Step 11: Select the appropriate system for implementation

Once the system has been optimised for functionality and cost, specific system characteristics are used as inputs to the detail requirements for the detail design phase of the SE life cycle, after which the system is implemented and evaluated in operation.

Two systems resulted from the acquisition process, performed in the real-world case study in Chapter 6, in addition to the original concept system, resulting in three physical systems. The three systems are (i) the original concept system as obtained from the mine, (ii) a system optimised for risk, and (iii) a system optimized for cost. All three systems were fully developed, manufactured and evaluated. The analysis and evaluation of these systems are discussed and presented in detail, using the ABR method, in Chapter 6.

5.4 Conclusion

Activity-based risk as a method to support acquisition of electronic safety equipment was proposed and defined in this chapter. This approach was developed with specific focus on development of electronic safety equipment in a mining environment.

Important characteristics of the ABR acquisition process are summarised below, namely that the process:

- Is a relativistic approach for comparison of different technologies in an integrated operational environment;
- Addresses risk and cost reduction by following an iterative design, simulation and evaluation approach using a functional framework;
- Introduces human error using risk scores and profiles that define human performance (from which probability distributions are derived);
- Translates risk to understandable operational response measures that are measured from simulations;
- Provides a balanced solution between technology (in terms of functional requirements) and human resources (in terms of risk performance);
- Provides a reference in a body of knowledge that is reusable and adaptable to accommodate system improvement over time;
- Gives visual results from simulations for decision support and, as ABR follows an SE process, brings together stakeholders from engineering and mining.

The ABR acquisition process addresses the discontinuity between acquisition and operations by focusing on a functional analysis in the preliminary design phase.

The acquisition method with ABR was developed from research challenges and solutions determined from the literature study presented in Chapter 4. Allocation of the acquisition method's characteristics to address required research solutions is presented in Table 8.

Table 8: Research solutions addressed by the ABR acquisition process

Research solutions / **The Activity Based Risk (ABR) Method**	Define detail system requirements in preliminary design	Follow an integrated approach	Follow a balanced approach (production, technology, safety, usability)	Follow integrated SE approach	Use functional analysis during preliminary design to obtain all relevant information.	Proactive risk management approach.	Follow a relativistic approach when comparing technologies	Introduce resource risk ratings to determine the operational effectiveness
1. Define AS-IS system design				X				
2. Do concept design for TO-BE system				X				
3. Perform functional analysis on candidate systems	X	X	X	X	X	X	X	
4. Build generic simulation model	X	X			X		X	
5. Set up volatility tables for human resources		X					X	X
6. Determine risk response measures		X					X	
7. Evaluate and compare models		X		X		X	X	X
8. Perform activity-based risk analysis		X	X	X		X		X
9. Identify high risk contributing activities		X	X			X	X	X
10. Optimise the system (risk and cost)		X	X			X	X	X
11. Select appropriate system for implementation		X		X		X	X	

Chapter 6
Winch signalling system case study

6.1 Introduction

This chapter presents a real-world case study where an electronic signalling safety system for winch scraper operations was analysed using the activity-based risk acquisition process, as from Chapter 5. This chapter shows all ABR acquisition process steps with details and results of each step.

As part of the case study, physical implementation of candidate systems was done. Implementation of the candidate systems validates the ABR philosophy and integrity of the ABR process developed in this research. Detail design and development of the physical systems are discussed and presented at the end of this chapter.

6.2 Case study definition

6.2.1 Winch signalling system background

In underground mines, scraper winches are used to clear ore from stopes and gullies after a blast. In scraper operations, risks are present that lead to injuries and fatal accidents.

In a study for SIMRAC (Safety in Mines Research Advisory Committee) by CSIR Miningtek and Camborne School of Mines, research shows that 9% of all underground accidents in the gold mining sector are associated with scraper winch systems. In the platinum sector, this value is lower at 5% [24].

Typical scraper winch accidents / hazards identified are as follows [24]:

- Rope related accidents where workers are in contact with a rope;
- Eyebolt / Snatch block (detach) related accidents, typically where an eye-bolt comes loose during scraping operations;
- Winch / Drum related accidents;
- Scraper / Scoop related accidents that occur in the path of the scraper.

The accidents related to these hazards are shown in Table 9 below.

Table 9 : Scraper winch related accidents [24]

Hazard	Platinum mines (%)	Gold Mines (%)
Rope	31%	30%
Snatch Block	23%	16%
Winch	24%	13%
Scraper / Scoop	21%	33%
Other	1%	8%

From the study by the CSIR [24] it was found that lack of proper communication (hence coordination) is one of the biggest contributors to scraper winch accidents.

A winch signalling safety system is used to reduce risks associated with underground scraper winch operations by addressing the lack of communication. The biggest drawback with mining safety systems is that, in many instances, their implementation results in decreased production and are therefore not accepted, not used, or simply bypassed by mine workers. The challenge with implementing such a safety system is to provide a safe working environment while maintaining prior levels of production.

The following sections discuss different configuration options (candidate systems and models) of winch signalling systems that were analysed and compared using the proposed ABR process. The conventional air whistle system is used as a reference (AS-IS) design for relativistic comparison.

6.2.2 Objective

The aim of this case study is to show that acquisition, including the design and implementation of a functionally optimal, risk-reduced solution can be done for a winch signalling safety system by following an activity-based risk acquisition process.

6.2.3 Process

The initial concept design of a winch signalling system (in the form of requirement specifications) for the initially proposed solution was provided by a mining group to address limitations of a conventional air whistle communication system (the AS-IS design). These requirements were established following the traditional approach as described in Chapter 3. This set of requirements was thus used as the initial concept design in the ABR process, after which the system was analysed in the ABR context, to provide alternative lower risk solutions.

In total, three candidate systems were developed and implemented. Utilization of these systems was used as validation of the ABR acquisition process in that the results from the ABR analysis agree with the results from practise.

6.2.4 Participants

A number of participants were identified in this study, including the following:

1. **Local mining groups**: Mining groups from the platinum and gold mining sectors were involved in the definition, evaluation and operationalization of the winch signalling systems. These include Anglo American Platinum, Impala Platinum, Anglo Gold Ashanti and Lonmin.
2. **Safety equipment development company**: A mining contractor participated to manufacture and supply safety equipment to the mines. This company funded development.
3. **Research team**: The research team consisted of three engineers (including the author and two electronic engineers) and a technologist, from the School for Electrical, Electronic and Computer Engineering, in the faculty of engineering at the North West University.

6.2.5 Roles and responsibilities

The local mining groups acted as the contract manager, and therefore the client in this case study. A mining group was responsible for the identification of the initial need for an improved winch signalling system, and provided a set of requirements to contractors for development. The mine was also ultimately responsible for the safety within mining operations and therefore responsible to test all developed equipment within controlled environments before utilisation in operations.

The development of a signalling system was funded by the local contracting company, allowing them to supply technology to the mine.

The research team acted as active participants and observers while developing the signalling systems according to the requirements from the mine. The research team performed the traditional hazard based product risk assessment in conjunction with the local contracting company, as presented in Appendix A, while all further system analysis, theoretical risk modelling and system development of further systems were performed by the research team. The author was responsible for risk modelling, risk analysis, development of risk controls, development management of safety equipment, evaluation of equipment before and during operation, and documentation

of all research done as defined in this thesis. In addition, activity-based risk was defined, analysed, and evaluated as part of the author's responsibility.

6.2.6 Results

This case study provides detailed results from the analysis of a winch signalling safety system in the ABR framework. The feedback from operations was used as validation for the ABR process, as this had to be consistent with the ABR model results.

This chapter contains a significant amount of data and may be considered tedious and overly detailed. However, the case study is presented to show all detailed steps that were followed in the analysis using ABR. Quite often, when risk analysis methods are presented, a theoretical method is proposed but practical implementation and examples are absent. That is, the "what" is shown, and not the "how".

The ABR process was initially developed when the first safety system was proposed by the mine and analysed by the research team, but ABR was not fully formalised at that stage. A formal definition of the process was done and was used to analyse all candidate models. The researchers were active participants and observers in the case study in order to obtain credible operational parameters. Interaction with the mining community contributed to the development of the ABR acquisition process. Therefore, development of ABR was done while systems were taken through detail design and implementation (all detail design and implementation were done by the research team).

6.3 Winch signalling system analysis

6.3.1 Conventional systems (ABR Step 1: AS-IS system)

The mine health and safety act of 1996 defines minimum requirements for signalling devices in scraper- / mono-winch operations. Regulations for communication systems are as follows (quoted *verbatim* from the act [12]):

- "Means are provided to forewarn persons of the intention to commence operating any scraper-winch or mono-rope winch;
- Means are provided for persons to signal to the operator, from any access point to the installation, to shut down the operation of the scraper-winch or mono-rope winch installation;

- Illumination of the moving parts of any winch so that they can be identified by persons;
- Winch starter box location to ensure ease of operation by the operator."

In most mines an air whistle system is currently being used to provide communication along gullies. This signalling device consists of an air whistle (or light bulb) which is activated by pulling a bell wire installed along the gully. The system allows mine personnel to communicate with the winch driver, and *vice versa*. Miners generate coded signals to inform a winch driver of actions that the miners need to take, and the winch driver informs miners on status changes at the winch (including winch start, stop, as well as safety and emergency conditions).

This is a fairly low-cost communication device, but has the following limitations, listed by [24]:

- An bell wire system provides one-way communication with no feedback given to the person initiating a signal from the gully;
- In some cases, a bell wire is not connected to the signalling device at the driver, resulting in signals along the gully not being communicated to the driver;
- Compressed air supply is not always connected to the signalling device (air whistle);
- The bell wire can be snagged or obstructed, especially in longer gullies;
- Gullies are not always straight, which poses a challenge for the installation of bell wire;
- Signalling devices can be defective or bypassed while it allows scraping to proceed;
- Incorrect installations are made where a bell wire is not installed on both sides of the gully and / or not to the entire length of a gully;
- Extreme noise caused by drilling operations results in the air whistle signals not being audible to the winch operator;
- There is no visible indication of system status.

Given the above shortfalls of the current system, a need was identified for a winch signalling communication device that uses modern, feature-rich technology.

The conventional air whistle system (AWS) is defined as the AS-IS system throughout this case study. It will also be referred to as the AWS or Option 1 throughout the text.

6.3.2 System requirements (ABR Step 2: Determine TO-BE system)

A South African mining group developed a specification for a new generation signalling device that adheres to the mine health and safety act of 1996, addressing shortfalls of the conventional air whistle system. The key requirements for this enhanced system are shown in Table 10 below. These requirements define core functions of the system.

Table 10: Enhanced electronic signalling system key requirements

	Winch signalling safety system – Requirements summary
1	The system will make use of a modular configuration with a control unit located at the winch itself with remote units along the gulley indicating the status of the system.
2	A pull wire configuration will be used for the exchange of signals. The same electrical cable used for powering the devices can be used as the pull wire.
3	Signalling (communication) should take place via audible and visual signals (alarm and robot system).
4	The winch signalling system should provide at all times for continuous indication at all entrances to the scraper path.
5	The system should provide communication along the whole of the scraper path including all areas between the scraper winch and the return rig of the scraper winch rope.
6	The system states (conditions) should be as follows: Safe, Prestart, Unsafe.
7	General signalling on the system should be possible in all states of the system.
8	Signalling (communication) should be possible on both sides of the scraper path (for centre gulley scraper winch installation).
9	A pre-start procedure is required before allowing scraper operations.
10	Once the prestart procedure (15 seconds) is complete, the unit enters the unsafe state.
11	Scraper winch operation is only allowed during the unsafe state. During the safe and pre-start states the winch operator does not have access to control the winch.
12	In the event of an emergency, it should be possible to interrupt the winch scraper operation. The interruption should be made possible by means of the pull cable, by any person in close proximity or within the scraper path of the scraper winch installation.
13	Condition (event) logging should be done to log all system events for at least the last seven days.
14	When signals are exchanged from remote units along the gulley, the position from where this signal was communicated should be shown on the control unit at the winch.
15	Access to the system should be restricted, while access is only allowed by means of a unique operator identification device.
16	The system should make use of a centralized power supply, and no voltage on the system should exceed 32V.
17	System diagnostics should be available for easy fault detection. The location of the fault should also be visible.
18	The signalling system should maintain a fail-to-safe operation.

The requirements above were used to define the new system (TO-BE) for analysis using the ABR process. This system is called the electronic signalling system and will be referred to as ESS or Option 2 throughout the case study.

6.4 System definition and functional analysis (ABR Step 3)

In this section, two systems are analysed and defined in terms of functionality. The first analysed system is the "AS-IS" system, described as the air whistle system above. The second is the proposed electronic signalling system defined by the requirements obtained from the mine (Table 10) – this is the TO-BE system.

A functional analysis is carried out in detail for both systems using ABR, including a system architecture, interfaces between the system and the environment (mechanical, electrical and operational), a general system layout, functional flow and states of all resources, definition of general system activities, followed by a resource allocation for each of the systems.

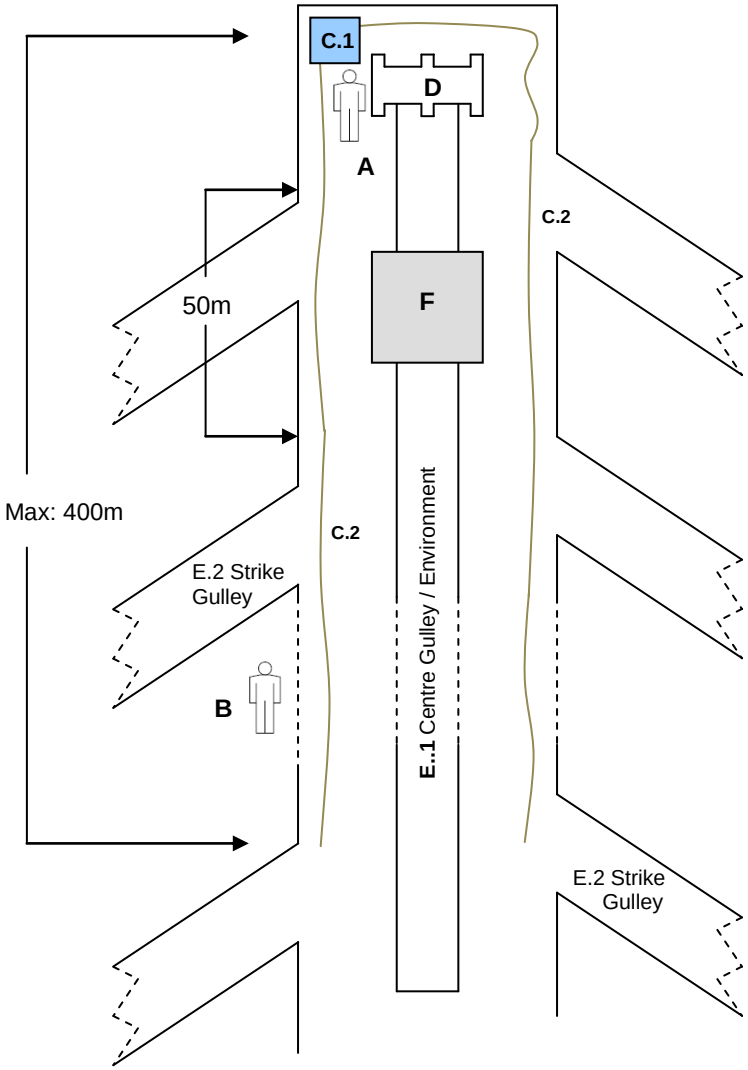
6.4.1 Option 1 – Air Whistle system (ABR step 3: AS-IS design)

This section presents the analysis and definition of the air whistle system (AWS).

6.4.1.1 System architecture (AWS)

The system architecture for the conventional air whistle system (AWS) is shown in Figure 25 on the next page. This illustration indicates all system resources and their interfaces.

The air whistle system makes use of an air whistle to communicate along a gulley. The winch driver can send signals along the gulley while miners crossing the gulley can pull the strain wire to signal to the winch driver. The system allows only for audible communication (at the winch driver) with no winch trip functionality.



A. Winch operator
B. Miner crossing the gulley
C. Air whistle system
C.1 Air whistle unit
C.2 Strain wire for signalling
D. Winch
E. Environment
E.1 Centre gulley
E.2 Strike gulleys
F. Scraper

Figure 25: Air whistle system architecture

6.4.1.2 System interfaces (AWS)

System interfaces between the resources are shown in the following figure, after which the interface definitions follow:

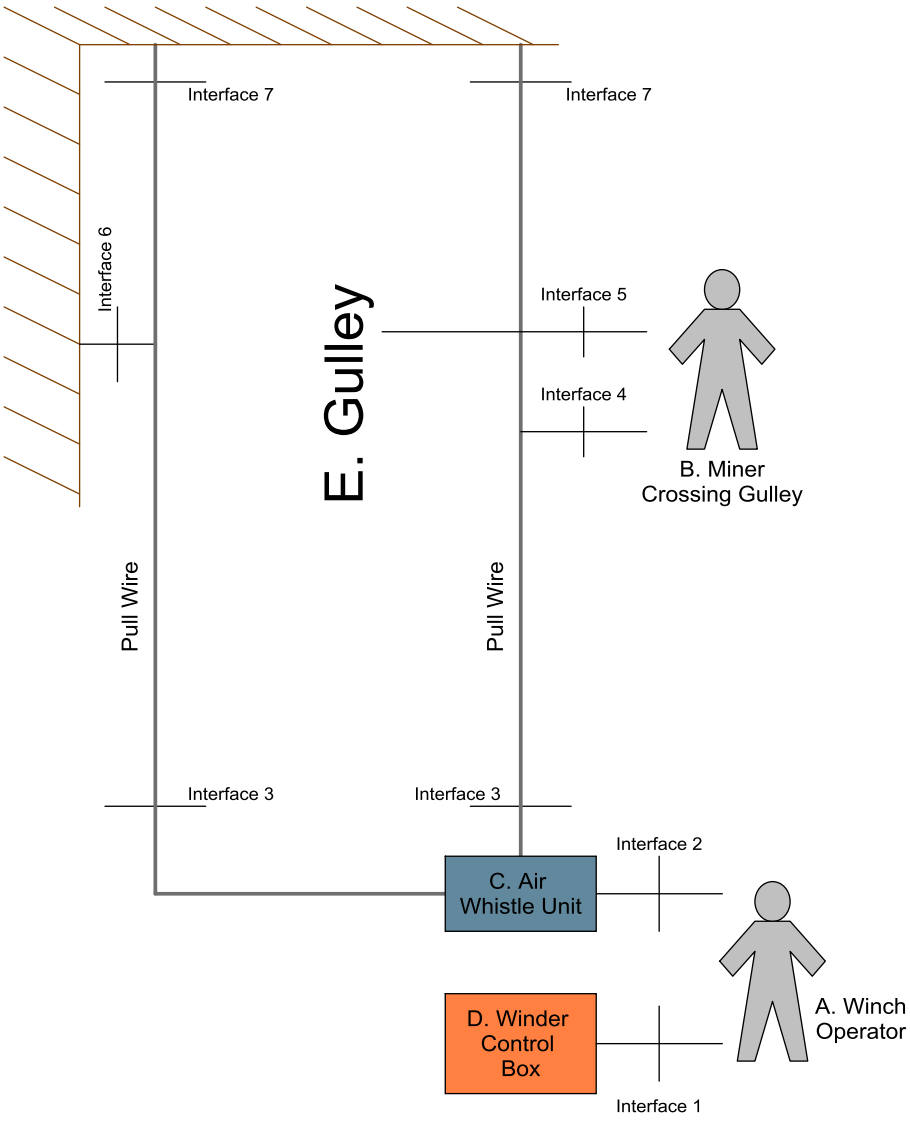


Figure 26: Air whistle system interface definition (AWS)

Interface 1 – Operator to winch control box interface

This is a human-machine interface between the operator and the winder control box. The following actions can be performed via this interface:

- Start the winch - The operator uses this interface to start the winch by activating the breaker.
- Stop the winch - The same beaker is used to remove power from the winch to stop it.

Interface 2 – Operator to air whistle unit interface

This is an audible human-machine interface from the air whistle unit to the operator. When the pull cable is pulled along the gulley, the air whistle system will sound.

Interface 3 – Pull wire connection

This is a mechanical interface. The pull wire is connected to pull switches of the air whistle unit to allow signalling from the gulley.

Interface 4 – Miner crossing / pull wire interface

Personnel working around and crossing the gulley must be able to pull the pull wire to generate signals to the winch operator. The pull wire should be easily accessible for personnel working along the gulley.

Interface 5 – Miner crossing / gulley state interface

This interface is used to determine the state of the gulley. The miner should determine whether the gulley is in safe, unsafe or prestart states. There is no specific indication by the AWS of the environmental state – this is done by the miner crossing by visual inspection.

Interface 6 – Pull wire support

Supports for the pull wire are required along the gully. This is necessary to guide the wire and relieve the strain on the pull switches which might cause nuisance pulls and signals.

Interface 7 – Pull wire termination

The pull wire should be terminated properly at the end of the gulley. This ensures tension in the wire to allow activation of the pull switch when the wire is pulled.

6.4.1.3 Resource functions and states (AWS)

Each of the functions or states of resources indicated in the system architecture as illustrated is shown and discussed in this section (Figure 25). Note that where human resources are applicable, functions are allocated. For the equipment and environment, states are defined. These states are typically driven by the human resource functions and interactions.

1A: Winch Operator functions (AWS)

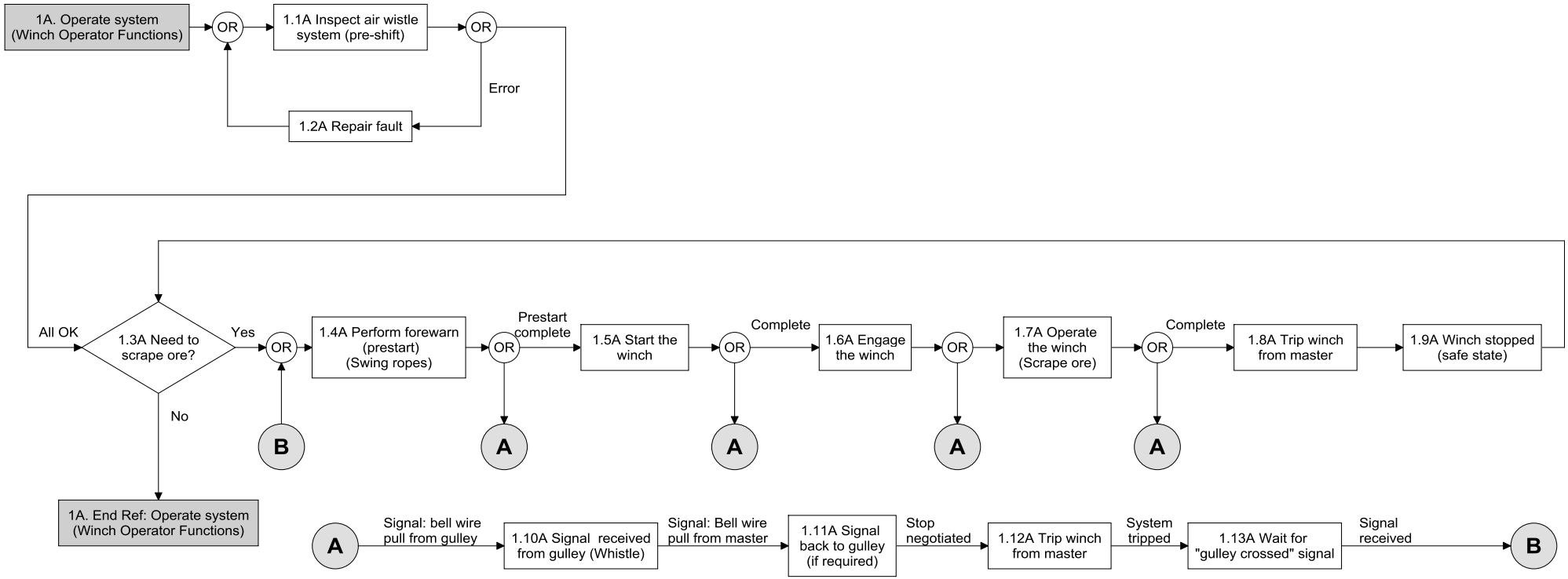


Figure 27: Winch operator functions (AWS)

1.1A Inspect air whistle system: A pre-shift inspection must be performed by the winch operator to ensure air is supplied to the air whistle system and that the air whistle system is functional.

1.2A Repair fault: If a fault is present, the fault should be addressed before the winch operator can proceed with operations. If it is a minor fault, it can be addressed by the winch operator, alternatively this fault needs to be repaired by a technician.

Note that, in the case of a signalling system error, the winch can still be started as the signalling system does not control power to the winch. There is no interface between the signalling system and the winch.

1.3A Need to scrape ore?: In this function, the winch operator must determine whether ore is present in the gulley that must be scraped. If ore is present, the winch operator should proceed with operations.

1.4A Do forewarn (prestart): This function is carried out by the winch operator to warn all miners in the area that the winch will be started shortly to scrape ore. This forewarn routine is carried out by the winch operator pulling / pulsing winch cables up and down along the gulley for a certain amount of time (using the winch itself).

1.5A, 1.6A, 1.7A – Do production: The do production procedure consists of the winch driver starting the winch. Thereafter the winch is engaged so that the winch can scrape ore along the gulley. This procedure is followed until all ore has been scraped from the gulley and can be interrupted by miners crossing the gulley via signals from the air whistle system.

1.8A Winch driver stops the winch: In this function the winch driver stops the winch. This is done if the production process is complete (a similar function exists in 1.11A for times when a winch stop is requested from the gulley).

1.9A Signal received from gulley: This signal is initiated from the gulley when miners crossing pull the pull cable. This signal is received by the winch operator via the audible interface. The winch operator should react to these signals accordingly.

1.10A Signal back to gulley: The winch operator can signal back to the gulley to allow for two way communication.

1.11A Winch driver stop the winch: The winch driver should stop the winch if this is requested from a miner that needs to cross the gulley.

1.12A Wait for "Gulley Crossed" signal: When the winch is stopped due to a request from the gulley, the winch operator should wait to allow the miner to cross the gulley. When a signal has been received from the miner that the gulley has been successfully crossed, the winch driver can proceed with operations.

1B: Miner crossing the gulley functions (AWS)

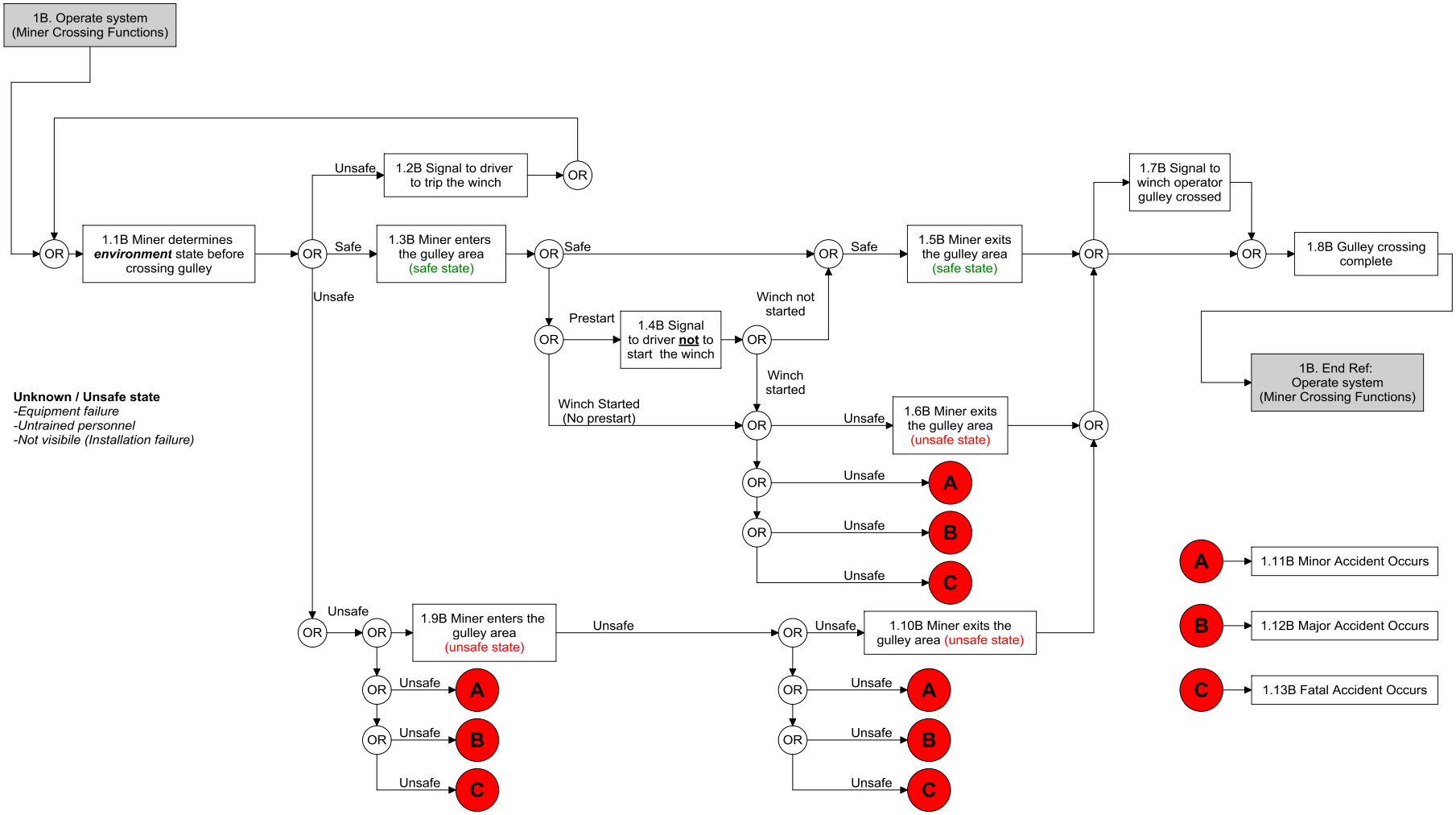


Figure 28: A miner crossing the gulley functions (AWS)

1.1B Miner determines environmental state before crossing the gulley: This function requires the miner to visually inspect the gulley to determine whether ore is being scraped, a prestart routine is being performed or whether the gulley is in the safe state. Once the state has been determined, the miner can act accordingly.

1.2B Signal to driver to stop the winch: If the state is determined to be unsafe or in the forewarn routine, the miner crossing needs to signal to the winch operator to stop the winch or forewarn procedure to allow the miner to cross the gulley. This signalling function is performed by pulling the pull cable of the air whistle signalling system.

1.3B Miner enters the gulley area (safe state): If the environment is in the safe state, the miner enters the gulley in this state during this function.

1.4B Signal to driver not to start the winch: When the miner is inside the gulley and a forewarn procedure is being executed by the winch operator, the miner signals to the winch operator to stop the procedure to allow him to cross the gulley.

1.5B Miner exits the gulley area (safe state): In this function the miner exits the gulley area when the environment is in the safe state.

1.6B Signal to winch operator gulley crossed: Once the gulley has been crossed, the miner should signal to the winch operator that the gulley has been crossed. This will allow the winch operator to proceed with production. Note that this function in the functional flow can also be skipped as it often happens that the miner crossing does not signal when the gulley has been crossed (Figure 28).

1.7B Gulley crossing complete: This function indicates that the process for the miner crossing the gulley has been completed.

1.8B Miner enters the gulley area (unsafe state): It is possible that the miner can determine the state of the environment incorrectly and still enter the gulley in the unsafe state. This could also happen when a careless miner crosses the gulley and does not take notice of the environment state.

1.9B Signal to the driver to trip the system: When the miner is inside the gulley, it is still possible to signal to the winch driver to stop the system. This could typically occur when the scraper bucket (danger) is approaching.

1.10B Miner exits the gulley area (unsafe state): In this function the miner exits the gulley when the gulley is in the unsafe state.

1.11B Minor accident occurs: When a miner is in the gulley in the unsafe state, it is possible that an accident can occur. This process block represents a minor accident.

1.12B Major accident occurs: When a miner is in the gulley in the unsafe state, it is possible that an accident can occur. This process block represents a major accident.

1.13B Fatal accident occurs: When a miner is in the gulley in the unsafe state, it is possible that an accident can occur. This process block represents a fatal accident.

1C: Signalling system (Equipment) operation states (AWS)

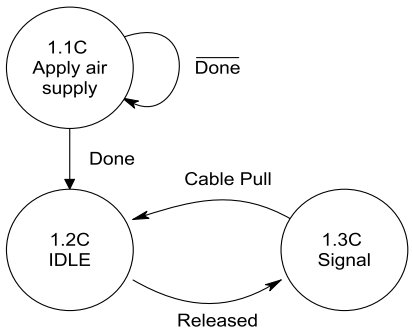


Figure 29: Signalling system states (AWS)

1.1C Apply air supply: Air must be supplied to the air whistle system to ensure operation. This is inspected by the winch operator during the pre-shift inspection.

1.2C Idle: This is the general state of the air whistle system.

1.3C Signal: When the pull cable is pulled, the pull switch on the air whistle unit allows the whistle to be activated.

1D: Scraper winch (Equipment) operation states (AWS)

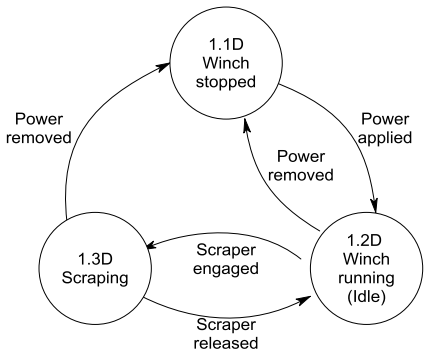


Figure 30: Scraper winch states (AWS)

1.1D Winch stopped: The winch is in the stopped state if no power is applied to the winch. This results in the environment being in the safe state.

1.2D Winch running (Idle): If power is applied to the winch, the winch motor will be running. Power is applied to the winch via the breaker at the winch control unit. In this state the scraper buckets are still not moving along the gulley but with the winch running, the environment is in the unsafe state.

1.3D Scraping: When the clutch is engaged while the winch is running, the scraper buckets will move along the gulley and ore will be scraped. The environment is still in the unsafe state.

1E: Gulley (Environment) states (AWS)

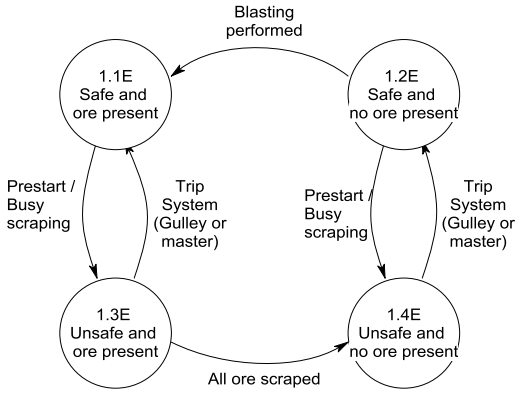


Figure 31: Gulley / environment states (AWS)

1.1E Safe and ore present: In this state the environment is in a safe state (no winch running) while ore is present.

1.2E Safe and no ore present: This state is entered once scraping operations have been completed and no more ore is present with the winch being stopped.

1.3E Unsafe and ore present: When ore is being scraped, the system will be in this state.

1.4E Unsafe and no ore present: If the scraper winch is scraping but no more ore is present, this state will be entered. This results in an unsafe environment and should occur less frequently.

6.4.1.4 AWS resource allocation

The resource allocation is performed for each of the resources in the AWS to map their corresponding states / functions for all generic system activities. This allocation for the air whistle system is shown in Table 11 on the following page.

The resource allocation is performed where the functions / states of each of the resources defined in the preceding section, are mapped for a specific system task / activity. The primary resource functions directly contributing to a specific activity being executed are highlighted. In the cases where multiple primary resource functions exist, there will be a defined interface between these resources. The possible states / functions for the remaining resources are listed for each activity, although these resources are not acting directly to perform a specific system task – therefore, they are treated as secondary resources for a specific activity.

Some activities are defined which are not applicable to this specific system, as obtained from an analysis of the more complex electronic signalling system. These activities are listed below, as this set of activities covers the complete range of system activities used in alternative system configurations discussed in the following sections of this study. Doing so allows a comprehensive comparison between all concept systems defined in the ABR process.

Table 11: Resource allocation for the air whistle system (AWS)

General Activities / Resource functions	Activity 1: Do pre-shift inspection	Activity 2: Identify if ore should be scraped	Activity 3: Determine environment state	Activity 4: Perform prestart	Activity 5: Trip prestart from master	Activity 6: Trip (stop) winch from master (driver)	Activity 7: Trip prestart from gulley	Activity 8: Trip winch from gulley	Activity 9: Start the winch	Activity 10: Scrape ore	Activity 11: Signal from gulley	Activity 12: Wait for gulley to clear	Activity 13: Investigate trip	Activity 14: Reset System
1A Winch Driver Functions (Human)	1.1A	1.3A	1.1A – 1.13A	1.4A	NA	1.11A	1.4A	NA	1.5A	1.6A, 1.7A	1.9A, 1.12A	1.12A	NA	NA
1B Miner Crossing Functions (Human)	1.1B, 1.3B, 1.5B, 1.7B	1.1B, 1.3B, 1.5B, 1.7B	1.1B	1.1B, 1.3B, 1.5B, 1.7B	NA	1.1B, 1.2B, 1.8B – 1.13B	1.4B	NA	1.1B – 1.13B	1.1B – 1.13B	1.2B, 1.6B, 1.9B	1.3B – 1.7B	NA	NA
1C Signalling System Functions (Equipment)	1.1C - 1.3C	1.2C	1.1C - 1.3C	1.2C	NA	1.1C, 1.2C, 1.3C	3C	NA	1.1C, 1.2C, 1.3C	1.1C, 1.2C, 1.3C	1.3C	1.2C, 1.3C	NA	NA
1D Scraper Winch operation functions (Equipment)	1.1D	1.1D	1.1D – 1.3D	1.1D	NA	1.1D	1.1D	NA	1.2D	1.3D	1.1D – 1.3D	1.1D	NA	NA
1E Environment / Gulley states (Environment)	1.1E, 1.2E	1.1E, 1.2E	1.1E - 1.4E	1.1E, 1.2E	NA	1.1E, 1.2E	1.1E	NA	1.3E	1.3E	1.1E - 1.4E	1.1E, 1.2E	NA	NA

6.4.1.5 Air whistle system functional analysis summary

The functional analysis of the air whistle system defines the system in terms of its architecture, interfaces and all possible states and modes. The resource allocation clearly indicates (highlighted in grey) the primary resources and the interaction between these resources for the complete set of system functions. The resource allocation further indicates the critical resources for the system – from Table 11, it is clear that the winch operator is the most critical resource as he (typically, a male operator) interacts with the most functions. The signalling system is a critical resource, while the table indicates that there is limited interaction from the miner crossing the gulley toward the safety system under consideration (AWS).

6.4.2 Option 2 – Electronic Winch Signalling System (ABR step 3: TO-BE design)

The electronic winch signalling system (ESS) option is defined to meet all requirements as set out in Table 10. This is a new system (TO-BE) that should be developed to replace the conventional air whistle system currently used in scraper winch operations. A functional analysis for this system is conducted in this section. This also includes the proposed system architecture, system interfaces, functional flow and resource allocation for the system.

6.4.2.1 System architecture (ESS)

The system architecture for the electronic winch signalling system is shown in Figure 32 below. This illustration indicates all system resources as part of the basic architecture of the proposed winch signalling system. This is a typical underground scenario with the control box situated at the winch, operated by the winch operator, while signalling units (slave units) are spaced down both sides of the gulley at 50 metre intervals.

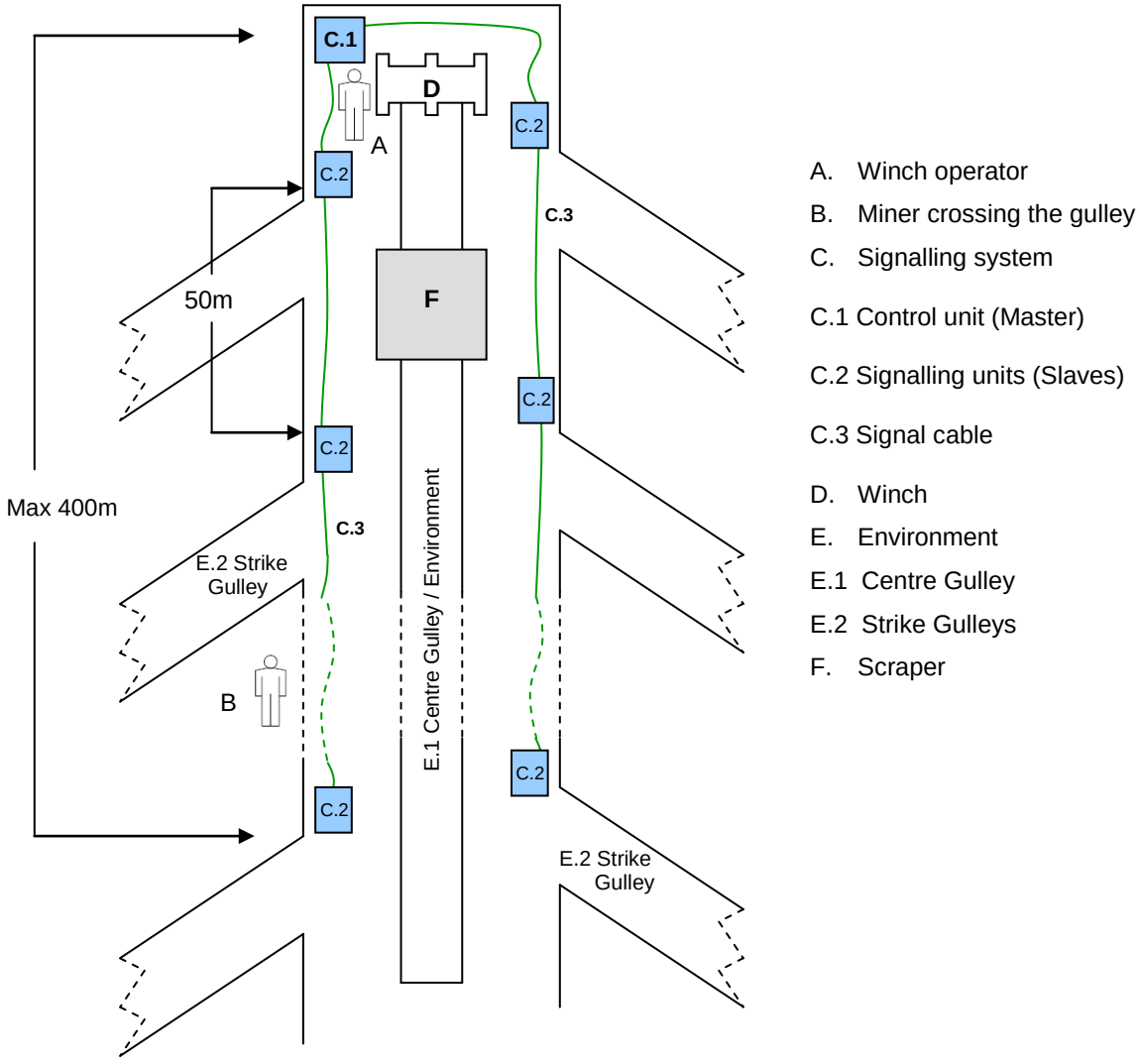


Figure 32: Electronic winch signalling system architecture (ESS)

The system consists of a master unit, with a controlled interface that allows access to winch functions. The system is also supported by slave units along the gulley for audible and visible communication to and from miners. Each slave unit is equipped with an LED bezel display and audible buzzer for system state indication along the gulley.

The master control unit and slave units are interconnected with electrical pull cables, also for signalling along the gulley.

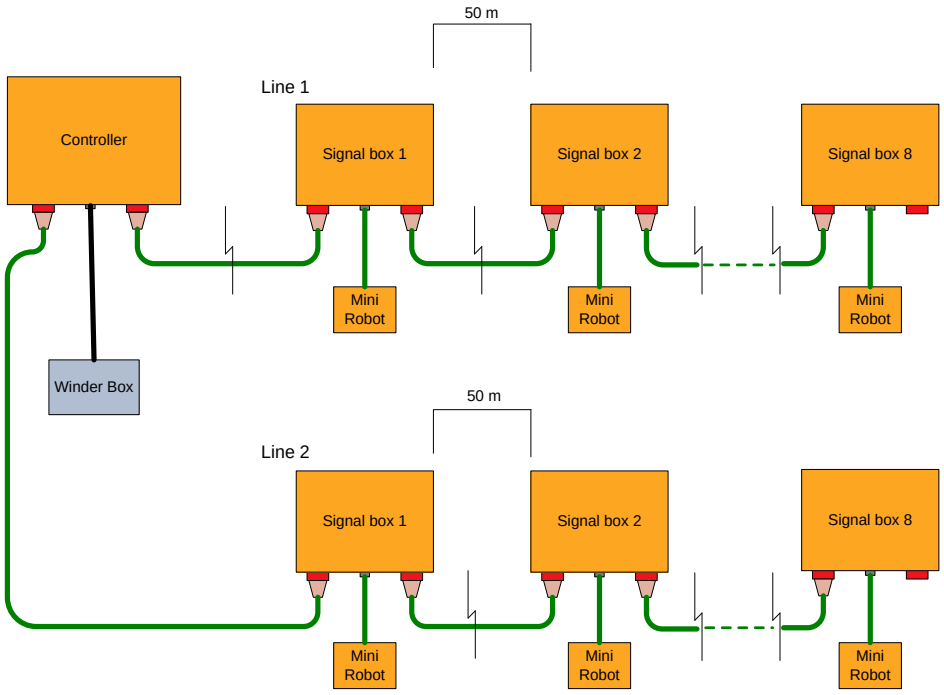


Figure 33: Electronic signalling system general layout (ESS)

The general layout of the system is shown in Figure 33. This shows how the master control unit is connected to the signal units (slave units) via the pull cable. The system design enables up to eight signalling units on each line, with the result that the system status can be displayed up to 400 metres along a gulley on both sides. Each slave unit can have a mini robot (with a buzzer and bezel) attached to it to indicate the status of the winch in a strike gulley. The connection to the winch control box is also shown.

6.4.2.2 System interfaces (ESS)

Interfaces identified between resources for the electronic signalling system are shown in Figure 34 on the next page. These include the electrical, mechanical and human-machine interfaces as discussed in the section that follows.

Interface 1 – Winch Operator to winch control box interface

This is a human-machine interface between the operator and the winder control box.

- Start the winch - The operator uses this interface to start the winch by activating the breaker. Note that this can only be done when the signalling system is in the unsafe state. Access to the circuit breaker is controlled via the master signalling unit using interface 3.

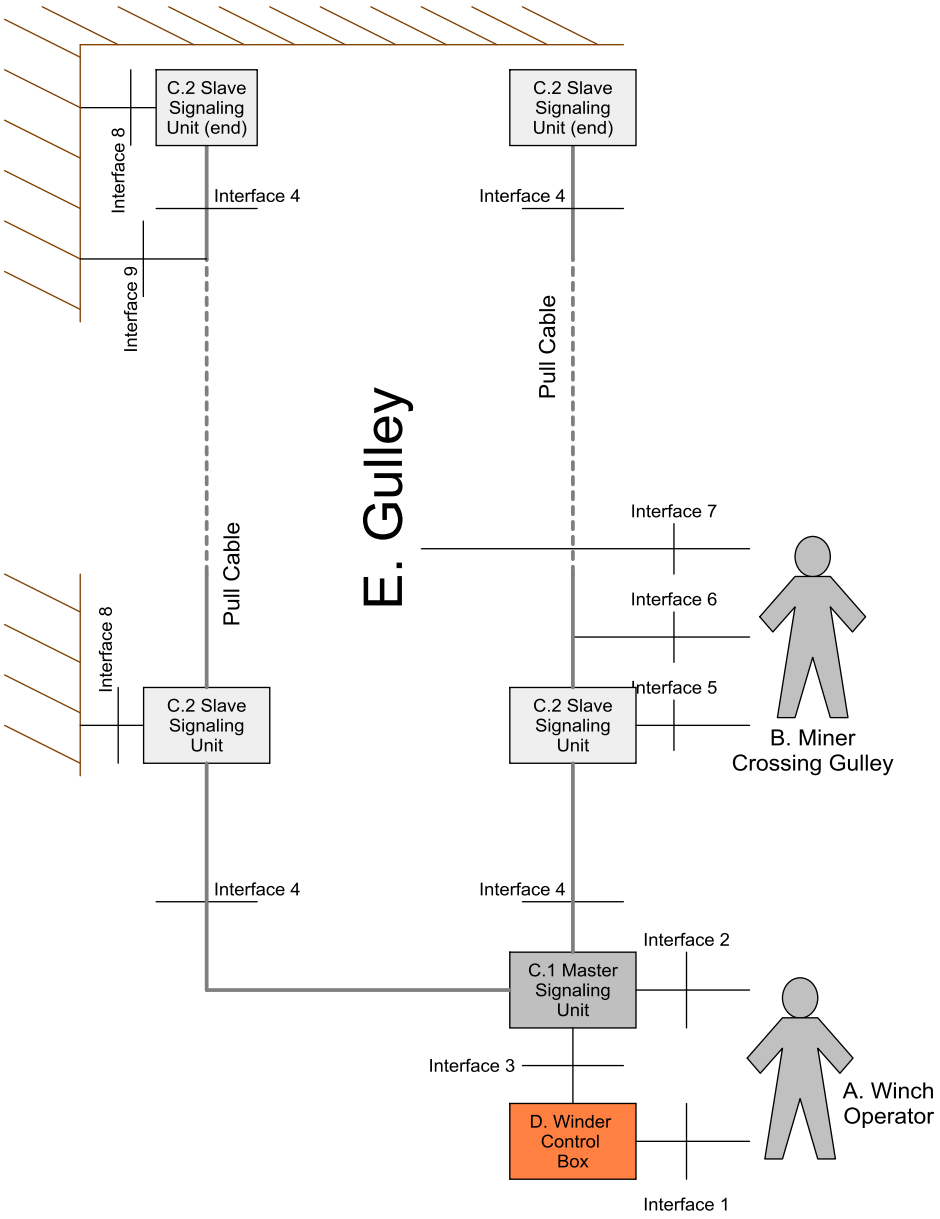


Figure 34: Electronic signalling system interface definition (ESS)

Interface 2 – Winch operator to master signalling unit interface

This is a human-machine interface with the following characteristics:

- Prestart – A prestart routine can be executed by pressing the prestart button on the master signalling unit when the unit is in the safe state. In this routine all bezels on all slave units along the gulley will flash red for 15 seconds, after

which the system will enter the unsafe state. This is a transitional activity as the system changes from low risk to high risk state;

- Signal button – The winch operator can press the signal button in any system state. When the button is pressed the bezels will be off while the buzzers on all units will sound. This button is used to communicate signals from the winch driver unit along the gulley;
- Bezel display – The bezel display consists of two visual status indications. Red indicates the unsafe state while the safe state is represented by green LEDs;
- Status display – The status display is used to indicate the status of each slave unit along the gulley. An LED is allocated to each slave unit, and this display is used to indicate the location of signals or trip events from the gulley. If an error occurs on a specific unit, this will also be indicated on this display.
- Buzzer – The buzzer is used for audible communication. The buzzer will sound when the system is used for signalling and also during the prestart routine.
- Key reader – Each control unit has a key reader that is used to control access to the unit, or to transfer logged events onto a key.

Interface 3 – Master signalling and winder control box interface

This is an electrical interface with the following characteristics:

- Power supply – Power is supplied from the winder control box to the signalling system. This is a low power source, typically 32 V_{AC}.
- Access control – A relay output is switched from the master control unit when the system is in the unsafe state. This dry contact output is configured to control the power to the winch breaker to allow (or disallow) the winch operator to start the winch.

Interface 4 – Interconnection and pull cables between signalling units

This interface consists of a 5-core interconnection cable, reinforced to withstand a harsh stope environment. The cable is interconnected for electrical connectivity between all signalling units, while it is also mechanically connected to pull switches of signalling units. The same cable is used as the pull cable for signalling.

Interface 5 – Miner crossing and slave signalling unit interface

This human-machine interface between the miner crossing and the closest signalling unit has the following characteristics:

- Bezel display – The bezel on each signalling unit shows the state of the signalling system and thus the environment state;
- Buzzer – When signals are communicated along the gulley, the buzzer will also sound.

Interface 6 – Miner crossing and pull cable interface

Personnel working around and crossing the gulley should be able to pull the pull cable to communicate with the winch operator. This can be a request to stop the winch, but the winch can also be tripped from this pull cable when pulled for longer than 2 seconds. The pull cable should be easily accessible to personnel working along the gulley.

Interface 7 – Miner crossing and gulley / environment interface

This interface can be used to further determine the environment state through visual inspection of the gulley itself (similar to the AWS). Note that the system state is indicated by interface 5.

Interface 8 – Mounting of signalling units

This is a mechanical interface defined by the physical mounting and installation criteria for the signalling units. The signalling units must be mounted so that they are clearly visible and should be spaced no more than 50 metres apart to ensure visibility of the system state along the gulley.

Interface 9 – Pull cable support

Supports for the pull cable are required along the gulley. This is necessary to guide the cable and relieve the strain on the pull switches which might cause nuisance pulls and signals.

6.4.2.3 System functions and states (ESS)

Each of the functions that must be performed by the resources indicated in the system architecture (Figure 32) is illustrated on the next page.

1A: Winch Operator functions (ESS)

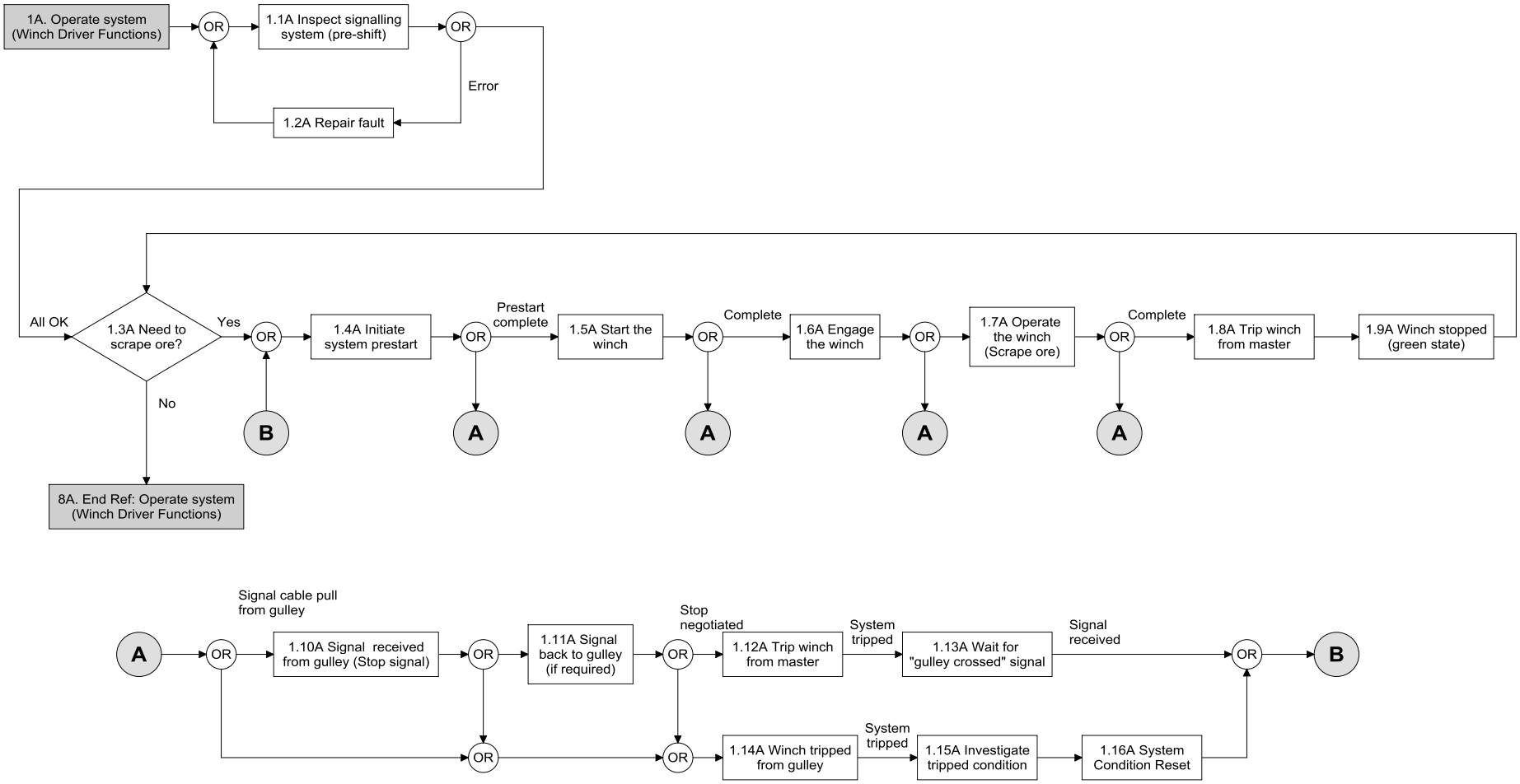


Figure 35: Winch operator functions (ESS)

1.1A Inspect electronic signalling system: A pre-shift inspection should be performed by the winch operator to ensure the signalling system is operational. Power should be supplied to the system and all signalling units need to be operational. The status of the signalling units is indicated on the led display on the master control unit of the signalling system.

1.2A Repair fault: When a fault is present, the fault must be addressed before the winch operator can proceed with operations. If it is a minor fault, it can be addressed by the winch operator, alternatively this fault needs to be repaired by a technician.

In the case of a signalling system error, the winch cannot be started as no power to the winch will be allowed. This is to ensure the system fails to a safe state.

1.3A Need to scrape ore?: In this function the winch operator must determine whether ore is present in the gulley that needs to be scraped. If ore is present, the winch operator should proceed with operations.

1.4A Initiate system prestart: This prestart routine is initiated by the winch operator by pressing the prestart button on the signalling system's control unit. This will initiate the prestart routine performed by the signalling system (for 15 seconds) to warn all miners in the area that the winch will be started shortly to scrape ore.

1.5A, 1.6A, 1.7A – Do production: The do production procedure consists of the winch driver starting the winch. Thereafter the clutch will be engaged, following which the winch can be operated. This procedure should be followed until all the ore is scraped from the gulley, but the procedure can be interrupted by miners crossing the gulley via signals and trips using the signalling system.

1.8A Trip winch from master: In this function, the winch driver will stop the winch. This will be done if all ore has been scraped during the production process. (Note that a similar function exists in 1.11A for times when a winch stop is requested from the gulley)

1.9A Signal received from gulley: This signal is initiated from the gulley when miners crossing pull the pull cable. This signal is received by the winch operator via the audible and visual interface of the signalling system. The location of the received signal is also indicated on the master display unit. The winch operator must react to these signals accordingly.

1.10A Signal back to gulley: The winch operator can signal back to the gulley to allow two way communication using the signal button on the master unit.

1.11A Trip the winch from master: The winch driver must stop the winch if this is requested from a miner (via the signalling system) that needs to cross the gulley. This can be done by holding the signal button for longer than 2 seconds to trip the system.

1.12A Wait for "Gulley Crossed" signal: When the winch is stopped due to a request from the gulley, the winch operator must wait to allow the miner to cross the gulley. When a signal is received from the miner that the gulley has been crossed, the winch driver can proceed with operations.

1.13A Winch tripped from gulley: The winch can be tripped from the gulley when the miner crossing pulls the signal cable for longer than 2 seconds when the system is in the unsafe state. The winch will stop immediately and the system will enter the tripped state.

1.14A Investigate tripped condition: The tripped condition must be investigated by the winch driver. In this function, the winch driver should locate the area from where the trip was initiated – this is indicated on the LED display of the master unit and the bezel of the specific signalling unit will also be flashing. The winch driver should walk to this specific signalling unit and investigate whether the surrounding area is safe, after which the tripped condition can be reset.

1.15A System condition reset: The trip condition can be reset on the signalling unit from where the trip originated. This is done by presenting the master key to the key reader of the tripped signalling unit. Only after this tripped condition is reset, can the winch operator proceed with operations. If the tripped condition is not reset, the system will not allow the prestart procedure to prevent further unsafe operations.

1B: Miner crossing the gulley functions (ESS)

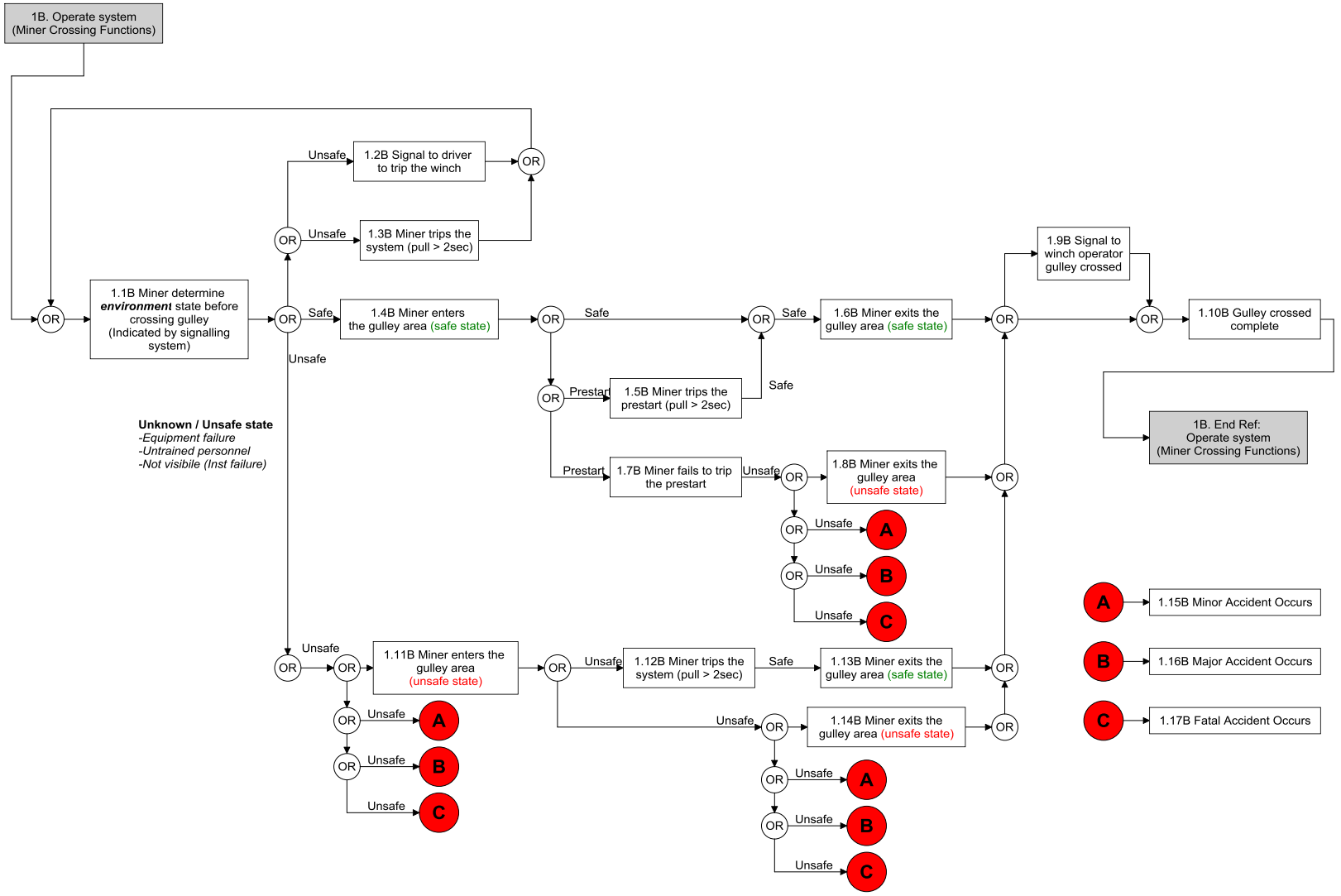


Figure 36: A miner crossing the gulley functions (ESS)

1.1B Miner determines environment state before crossing the gulley: This function requires the miner to visually inspect the gulley to determine whether ore is being scraped, a prestart routine is performed if the gulley exits the safe state. The electronic signalling system indicates this state via the status display on the bezels of all signalling units. Once the state has been determined, the miner can act accordingly.

1.2B Signal to driver to trip the winch: If the state has been determined to be unsafe, the miner crossing needs to signal to the winch operator to stop the winch to allow the miner to cross the gulley. This signalling function is performed by pulling the pull cable of the signalling system.

1.3B Miner trips the system: The system can be tripped from the unsafe or prestart states, to the safe state. This is done by the miner crossing when pulling the pull cable for longer than 2 seconds. The winch will stop immediately and the gulley will be safe for the miner to cross.

1.4B Miner enters the gulley area (safe state): If the environment is in the safe state, the miner enters the gulley.

1.5B Miner trips the prestart: When the miner is in the gulley and a prestart routine is being executed from the winch operator, the miner can trip the prestart state by pulling the pull cable for longer than 2 seconds.

1.6B Miner exits the gulley area (safe state): During this function the miner exits the gulley area when the environment is in the safe state.

1.7B Miner fails to trip the prestart: If the prestart routine is being executed with the miner inside the gulley and the prestart is not tripped within 15 seconds, the system will enter the unsafe state. This will result in a miner in the gulley, currently in the unsafe state, being exposed to hazard.

1.8B Miner exits the gulley area (unsafe state): In this function the miner failed to trip the prestart and exits the gulley when the gulley is in the unsafe state

1.9B Signal to winch operator gulley crossed: Once the gulley has been crossed, the miner must signal to the winch operator that the gulley has been crossed. This will allow the winch operator to proceed with operations. Note that in the functional flow (Figure 36) this function can be skipped as the miner crossing does not always signal when the gulley has been crossed.

1.10B Gulley crossed complete: This function indicates that the process for the miner crossing the gulley has been completed.

1.11B Miner enters the gulley area (unsafe state): It is possible that the miner can incorrectly determine the state of the environment and still enter the gulley in the unsafe state. This could also happen when a careless / untrained miner crosses the gulley and does not notice the environment state.

1.12B Miner trips the system: When the miner is inside the gulley, it is still possible to trip the winch. This could occur when the scraper buckets (i.e. danger) are approaching.

1.13B Miner exits the gulley area (safe state): Once the winch has been tripped from function 1.12B, the environment will be safe. This allows the miner in the gulley to exit the gulley in the safe state.

1.14B Miner exits the gulley area (unsafe state): In this function the miner exits the gulley when the gulley is in the unsafe state.

1.15B Minor accident occurs: When a miner is in the gulley in the unsafe state, an accident can occur. This process block represents a minor accident.

1.16B Major accident occurs: When a miner is in the gulley in the unsafe state, it is possible that an accident can occur. This process block represents a major accident.

1.17B Fatal accident occurs: When a miner is in the gulley in the unsafe state, it is possible that an accident can occur. This process block represents a fatal accident.

1.4C Safe state: In safe state, the system is safe to use and no power is supplied to the winch. Pre-start state can be entered by pushing the red button to start the winch. All the bezel lights will be green to indicate the safe condition.

1.4.1C Signal state: Same as 1.3.1C

1.5C Pre-start state: In the pre-start state all bezels flash red and sirens will sound simultaneously. This state lasts for 15 seconds (if not tripped) thereafter the system goes to the unsafe state and enables power to the winch.

1C: Signalling system (Equipment) operation states (ESS)

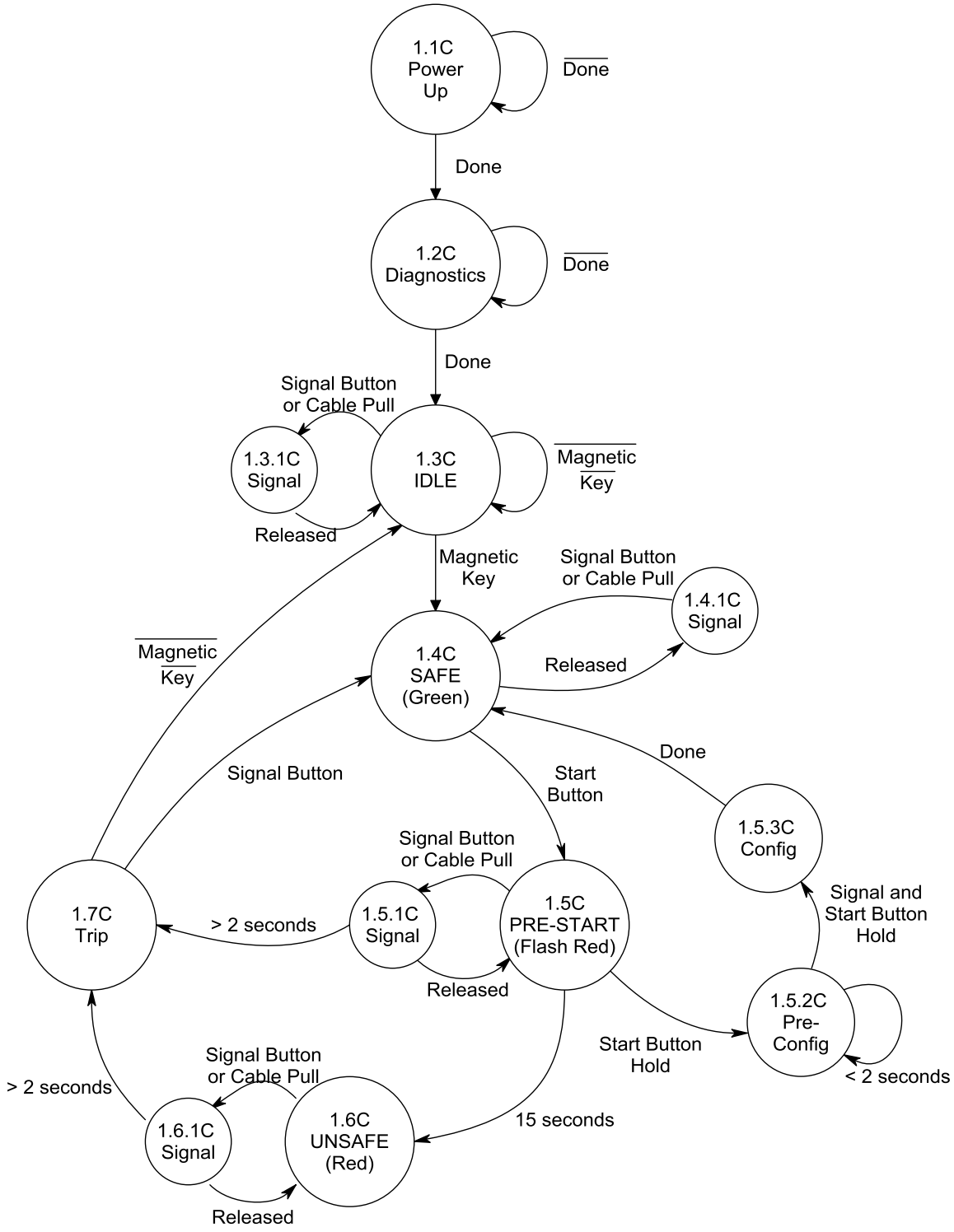


Figure 37: Signalling system states (ESS)

1.5.1C Signal state: The system enters the signal state if the green button on the master is pressed or if a cable is pulled along the line. The buzzers on all the units (control and signalling units) will sound while the bezel lights will be off for the duration of the cable pull or pushed button. A red LED on the master unit will flash to show from which signalling unit the cable has been pulled. If a cable is pulled (or the signal is button pressed) for longer than seconds the system will go to the trip state.

1.5.2C Pre-Config: This state is entered if the red start button is depressed (from entering pre-start state) and, after 2 seconds (on the third flash of the bezels), the green signalling button is pressed (while still holding the start button). Thereafter, when both buttons are released the system enters the configuration state.

1.5.3C Config: In this configuration state the system will find all the signalling boxes available on both lines. The LED display on the control unit will flash as it searches for the signalling units. Once the procedure has been completed, all the units that were found will be saved as the system's configuration, thereafter the system enters safe state.

1.6C Unsafe state: The unsafe state is entered once the pre-start state has been completed without any interruptions (>2 seconds signals). Power is supplied to the winch and the winch is able to operate.

1.6.1C Signal state: Same as 1.3.1C

1.7C Trip state: In this state, power to the winch is disabled. The appropriate red LED on the master unit will flash to show from which signalling unit the system is tripped. The trip should be investigated and reset on the corresponding signalling unit from where the trip originated. The system will reset to safe state if the access key is presented to the corresponding signalling unit.

1D: Scraper winch (Equipment) operation states (Option 2)

1.1D Winch stopped: The winch is in the stopped state if no power is applied to the winch. This results in the environment being in the safe state.

1.2D Winch running (Idle): If power is applied to the winch, the winch motor will be running. Power is applied to the winch via the breaker of the winch control unit. In this state the scraper buckets are still not moving along the gulley but, with the winch running, the environment is in the unsafe state.

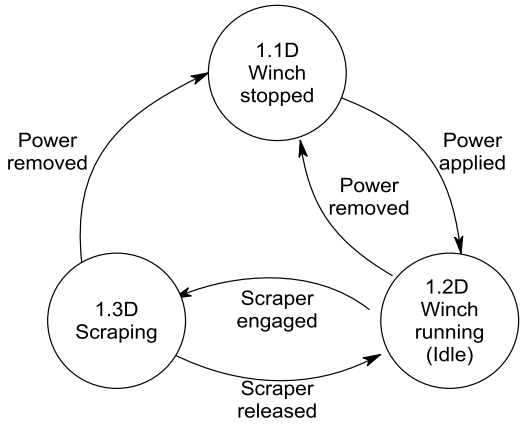


Figure 38: Scraper winch states (ESS)

1.3D Scraping: When the scraper is engaged while the winch is running, the scraper buckets will move along the gulley and ore will be scraped. The environment is still in the unsafe state.

1E: Gulley (Environment) states (Option 2)

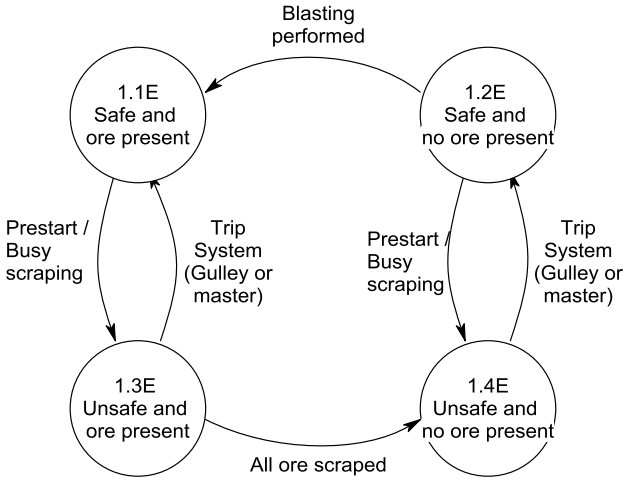


Figure 39: Gulley / Environment states (ESS)

1.1E Safe and ore present: In this state the environment is in the safe state (no winch running).

1.2E Safe and no ore present: This state is represented once scraping operations are complete and no more ore is present with the winch being stopped.

1.3E Unsafe and ore present: When ore is being scraped, the system will be in this state.

1.4E Unsafe and no ore present: If the scraper winch is scraping but no more ore is present, this state will be represented. This results in an unsafe environment.

6.4.3 Electronic signalling system resource allocation

The resource allocation for the electronic signalling system is shown in Table 12 on the next page. A general set of system activities is defined (the same set of activities used for the air whistle system in Option 1). Each of the resource functions / states is mapped for a specific system activity. Again, high risk resource functions / states are indicated by highlighted (in grey) blocks. These are critical resources required for specific system tasks, while the possible functions / states are indicated for the remaining resources.

6.4.3.1 Functional analysis summary of the electronic which signalling system

The functional analysis carried out on the electronic winch signalling system defines the system in terms of its architecture and all possible states and modes. The resource allocation clearly indicates (highlighted in grey) the primary resources and their interaction for the complete set of system functions.

The resource allocation (Table 12) indicates that the critical resources for the system are the winch operator together with the electronic signalling system as these resources act as primary resources throughout most of the system activities. This indicates that there should be a definite interface between these two resources. The miner crossing also acts as a critical resource in system activities, with the result that interfaces between the miner crossing and the electronic signalling system should be clearly defined.

Table 12: Resource allocation for the electronic winch signalling system (ESS)

General Activities / Resource Functions	Activity 1: Do pre-shift inspection	Activity 2: Identify if ore should be scraped	Activity 3: Determine environment state	Activity 4: Perform prestart	Activity 5: Trip prestart from master	Activity 6: Trip winch from master (driver)	Activity 7: Trip prestart from gulley	Activity 8: Trip winch from gulley	Activity 9: Start the winch	Activity 10: Scrape ore	Activity 11: Signal from gulley	Activity 12: Wait for gulley to clear	Activity 13: Investigate trip	Activity 14: Reset System
1A Winch Driver Functions (Human)	1.1A	1.3A	1.1A – 1.16A	1.4A	1.11A	1.8A	1.5A, 1.6A, 1.7A, 1.9A - 1.11A, 1.13A	1.13A	1.5A	1.6A, 1.7A	1.9A, 1.12A	1.12A	1.14A	1.15A
1B Miner Crossing Functions (Human)	1.1B, 1.4B, 1.7B, 1.9B	1.1B, 1.4B, 1.7B, 1.9B	1.1B	1.1B – 1.7B, 1.9B	1.1B, 1.2B, 1.4B, 1.5B, 1.6B, 1.9B	1.1B – 1.3B, 1.10B – 1.16B	1.5B	1.3B, 1.6B, 1.12B	1.1B – 1.3B, 1.8B – 1.16B	1.1B – 1.3B, 1.8B – 1.16B	1.2B, 1.5B, 1.8B, 1.11B	1.4B – 1.9B	1.1B, 1.4B, 1.8B, 1.0B, 1.14B	1.1B, 1.4B, 1.8B, 1.10B
1C Signalling System Functions (Equipment)	1.2C	1.3C	1.1C – 1.7C	1.5C	1.5.1C	1.7C	1.5.1C	1.7C	1.6C	1.6C	1.3.1C, 1.4.1C, 1.5.1C, 1.6.1C	1.3.1C, 1.4.1C, 1.5.1C, 1.6.1C	1.7C	1.3C
1D Scraper Winch operation functions (Equipment)	1.1D	1.1D	1.1D – 1.3D	1.1D	1.1D	1.1D	1.1D	1.1D	1.2D	1.3D	1.1D – 1.3D	1.1D	1.1D	1.1D
1E Environment / Gulley states (Environment)	1.1E, 1.2E	1.1E, 1.2E	1.1E – 1.4E	1.1E, 1.2E	1.1E	1.1E, 1.2E	1.1E	1.1E	1.3E	1.3E	1.1E – 1.4E	1.1E, 1.2E	1.1E	1.1E, 1.2E

Although it is clear from the functional analysis and system definition performed on these two systems (AWS and ESS) that the electronic signalling system provides a much safer working environment compared to the conventional system. It should be asked what the impact on operations will be which, in turn, will have an impact on production. This will determine whether the system will be accepted by mining operations because, when a system is forced upon operations, it will be bypassed or even vandalised.

In the following section, a detailed system analysis, following the ABR process, will be carried out to determine the impact of the two systems on safety and production.

6.5 System analysis (synthesis and design)

The two defined signalling systems (AWS and ESS) will be analysed in this section. In this analysis it is necessary to determine the system's impact on environment (operational) safety but also production. These two factors will represent the response measures related to risk, namely safety and production for each of the defined systems.

The system analysis is performed by simulating both systems in terms of general operations. A simulation for each system is constructed in SIMIO after which specific results can be determined. The SIMIO simulation model allows determination of impact of each of the functions defined in the system with the focus on safety and production. From this information, the system can be risk- and cost-reduced in terms of specific risk parameters.

6.5.1 Model simulation - building the simulation model (ABR Steps 4 – 10)

The SIMIO simulation software provides an object-oriented approach to rapid modelling and the flexibility to model complex systems [71]. Using this platform, two separate simulation models had to be constructed to represent the Option 1 (Air whistle system) and Option 2 (Electronic winch signalling system) systems.

The aim of the simulation is to "optimize" the design for safety and production. It is common that, in general safety systems, production is almost always compromised when safety is introduced. Thus, it is imperative to find the optimal solution where the safety in the system is at an acceptable level while maximum *safe* production output is achieved – safety will thus always be a constraint.

The functional flow from above shows all possible defined states for the resources (within the scope of the system). The resource states for humans (winch operator and miners crossing the gulley) are determined by the remaining resource states

which are the equipment (signalling system and scraper winch itself) and the environment (the states of the gulley). In the functional flow, all possible routes (decisions) for the winch operator and miner crossing the gulley are shown. This allows the translation of functional flows to event trees for each system.

The aim of an operational simulation is to determine a safe, productive system using safety and production as the risk drivers for each system by integrating safety resources and production resources.

The approach followed for this research will be to find production time and hazardous exposure time for each system by means of simulation.

To find the optimal solution, both the air whistle system (AWS) and electronic signalling system (ESS) will be simulated with the same initial environment parameters. Variability is introduced into the model resulting in deviations in real-world scenarios. To implement the same deviation in both models, it is important to make the same assumptions for both models. As this is a relativistic study, only the difference between results of the two models will be evaluated and used for optimisation. Thus, if the same deviation occurs in results of both models, this deviation will not be present in the compared results once the model results are compared.

The simulation model, definition of volatility tables, implementation and results are discussed in the following sections.

6.5.2 Create generic simulation model (ABR Step 4)

6.5.2.1 Human resource states

A generic simulation model was created that incorporates functions of both the air whistle and electronic winch signalling systems. The simulation can be configured to perform functions and scenarios of each system by setting input properties for the model. A graphical representation of the generic model is shown in the figures below (Figure 40 and Figure 41):

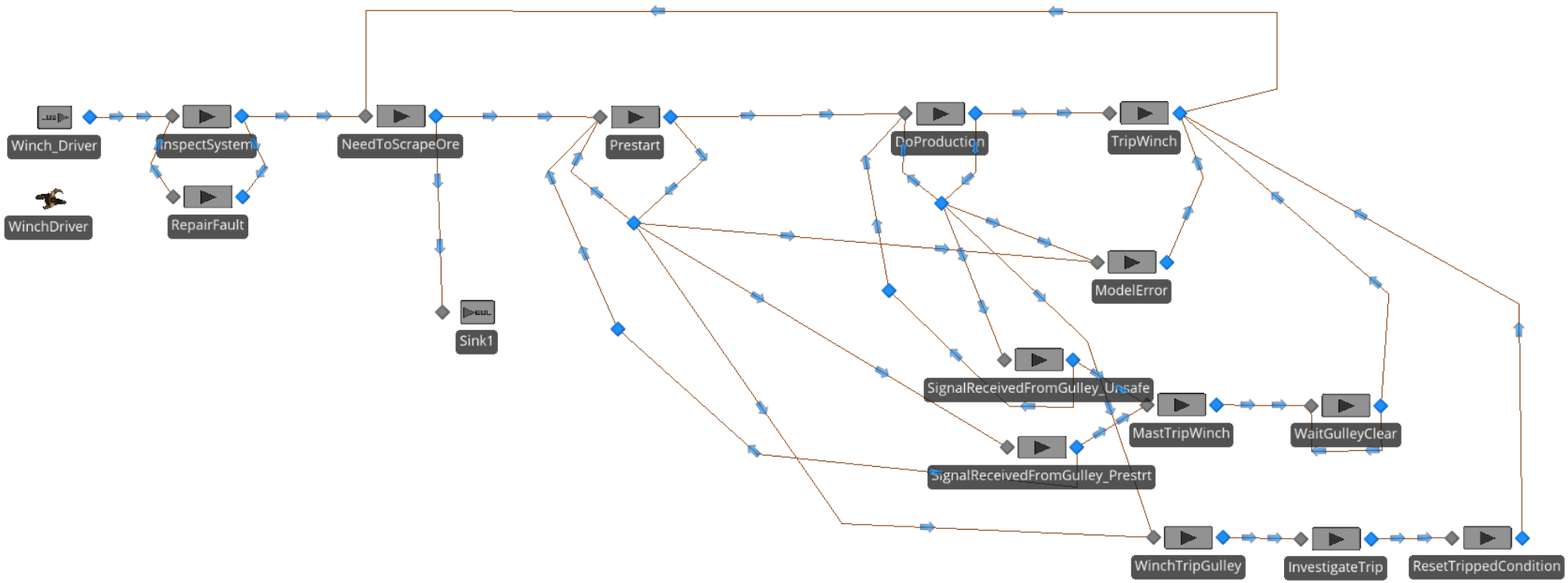


Figure 40: Winch operator generic simulation model layout

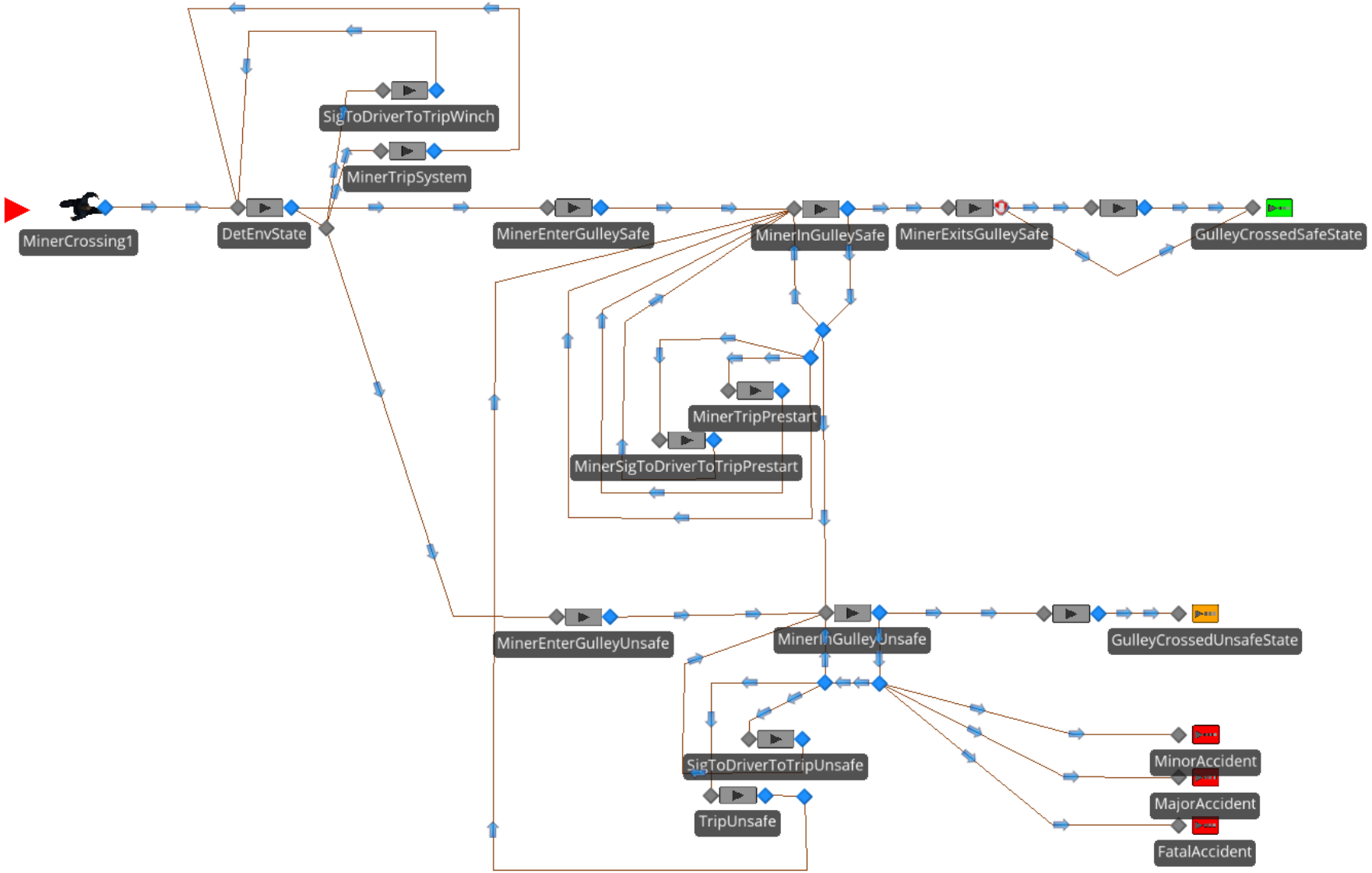


Figure 41: Miner crossing the gulley generic simulation model layout

The generic simulation model layout for the winch operator (Figure 40) shows the required functions for both systems as defined in Figure 27 and Figure 35 from the functional analysis. For the air whistle system, the "*WinchTripGulley*", "*InvestigateTrip*" and "*ResetTrippedCondition*" processes are not relevant and the paths to these processes will be disabled for the air whistle system.

The functions *1.5A Start the winch*, *1.6A Engage the winch* and *1.7A Operate the Winch* are combined into one process for the simulation, namely "*Do Production*". This is done for both system configurations (AWS and ESS), as the procedures followed (and risks involved) in these three steps are the same. Combining the three functions can be done as no differences between the two systems exist for these functions.

The generic simulation model for the miner crossing the gulley is shown in Figure 41. This implementation relates to functions as described in the functional analysis for this resource for both systems (see Figure 28 and Figure 36). Again, this generic model allows disabling of non-relevant functions and reconfiguration of the routes followed by entities for each signalling system type.

Implementation of both human resources, as described above (Figure 40 and Figure 41) is integrated into one model. Although there are no physical paths (connections) between these two resources in the model, the state of the equipment and environment determine the routes followed for each of the resource instances. In each resource instance, these equipment and environment states can change which, in turn, will have an influence on both human resource instances. The implementation of the equipment and environment states are further discussed in the following two paragraphs.

The representation of the simulation model layout corresponds directly with the functional flows as determined in the functional analysis. This emphasises the importance of the functional analysis when following the ABR process, as the functional analysis can be directly translated to a simulation model when a comprehensive analysis has been completed.

6.5.2.2 Equipment states

The implementation of the equipment states is done using state machines defined in the functional analysis. The state definitions from Figure 37 were used, representing the electronic signalling system (ESS), for the equipment states in the generic model implementation. Note that the equipment states for the air whistle system (Figure 29) are limited but these limited states overlap with corresponding states in the electronic signalling system. Again, these parameters are set as part of the input parameters to the generic model to define each system type.

6.5.2.3 Environment states

The environment states are the same for both the AWS and ESS systems, as shown in Figure 31 and Figure 39. As the focus of the simulation model is to determine the hazardous exposure time and production time of each system, the simulation will be run for states where ore is present during safe and unsafe operations. The safe and unsafe environment states are driven by the signalling system for each option, so no additional implementation is required as inputs to the simulation model.

6.5.3 Modelling using different people resource types (ABR Step 5)

Modelling a real-world scenario becomes challenging when people are used as resources. It is clear that equipment has defined states and conditions that can be predicted according to the equipment design. Because humans are not machines, human actions cannot be predicted with certainty and human actions are more volatile and dependent on various human factors. As seen in the literature study, these factors include training, automation and new technology, work procedures, task feedback, ergonomic considerations, workload, organizational and psychosocial factors, use of rules, personality, tendencies under stress, etc [41].

By adding volatility of human actions (error) to the model, 5 different human risk levels are defined. This allows the simulation model to be run for each system for each risk level of human used as a resource. A human risk level is defined by setting probabilities of various routes followed in workflows (behaviour) of the model, taking the interfaces and information available to the human into account. These probabilities are set for actions where human resources can deviate, and thus follow different routes through the workflow trees. These actions and probabilities are determined in the following two sections by construction of volatility tables for all human resources (ABR Step 5).

6.5.3.1 Resource 1A: Winch driver volatility table definition (AWS and ESS)

The main focus of the winch driver is to scrape ore. When introducing a safety system into this environment, it is necessary to determine the impact on the environment safety given the safety actions required by the winch driver. Therefore, there is a need to determine all activities where an action is required from the winch driver that will change the environment state from unsafe to safe. For both systems, a function exists where the winch driver should trip the system when requested from the gulley. This action relates to Activity 5 (*Trip prestart from Master*) and Activity 6 (*Trip winch from master*) of the general system activities identified in the resource

allocation of the functional analysis (see Table 11 and Table 12). These activities have a direct impact on the safety of the environment. The volatility in the execution of these activities will be added to the simulation model, according to the values shown in Table 13. Note that a 5% failure rate is selected for Activities 5 and 6, as there will be some form of error even for a low risk level winch driver. The failure rates for these activities increase as the resource's risk score increases. The 75% failure rate is selected for the highest risk type driver (type 5).

A further activity identified that will also have an impact on the system is Activity 12 (*Wait for gulley to clear*). In this activity, the miner crossing the gulley needs to signal to the winch driver that the crossing has been completed, but the driver will eventually proceed with operations if this signalling is not sent by the miner crossing. A timeout value is implemented for this activity and the deviation for this task will also depend on the risk level of the winch driver. The timeout values will not be fixed and are dependent on the risk level of the operator. These values and their deviations are shown in Table 13. (Deviations are introduced by the use of a triangular deviation function, where three values are defined. These values are the minimum value, the average value, and the maximum value. Random samples in this range will be drawn from a sampled population in simulation runs. The deviation values will be the same for both system options for Activity 12. Note that the average timeout value is set to be 60 seconds, as this time should allow more than enough time for the miner to cross a gulley. Typically, the higher a risk level of a human resource, the higher the deviation will be from the norm. The deviation values are selected to increase as the resource risk level increase.

Another safety-critical action required by the winch driver is initiation of the prestart task (Activity 4: *Do prestart*). In Option 2 (ESS), this task is enforced by the system, with the result that the winch cannot be started without going through the prestart procedure. In Option 1 (AWS), this task is not enforced and the duration is not fixed (user dependent). Thus, the winch driver can bypass this function, or deviate from the normal, expected execution time. The winch driver volatility of the prestart is also introduced in the model by using a random triangular function. The minimum, mean and maximum values represented for the winch driver type is shown in Table 13. The norm value for this prestart is set to be 15 seconds with a deviation added. Note that the execution time of Activity 4 decreases with a higher risk type driver, because the tendency is to complete the prestart routine so as to proceed with production.

The conceptual design of Option 2 (ESS) introduces additional functionality where a tripped condition along the gulley needs to be investigated by a winch driver. This

results in the winch driver walking up to the point where the trip was initiated and resetting the system at that point (while investigating that the environment is still safe) before scraping can proceed. This procedure is represented by Activity 13, and the time for these actions will be dependent on the risk level of the winch driver. The time taken for this activity will also be dependent on the location of the trip along the gulley, but an average time was set for each winch driver type, with deviation in both directions. These times are presented (in minutes) in Table 13.

Table 13: Winch driver type volatility table (AWS and ESS)

Resource risk level: **Winch driver**	**Activities 5 and 6 action:** **Winch driver trips system when requested**	**Activities 5 and 6 alternative action:** **Winch Driver fails to trip system when requested**	**Activity 12 deviation:** **Wait for gulley to clear timeout**	**Activity 4 deviation:** **Winch driver does prestart**		**Activity 13 deviation:** **Winch driver investigates tripped condition**	
System configuration	AWS and ESS	AWS and ESS	AWS and ESS	AWS	ESS	AWS	ESS
Deviation function	Probability Based	Probability Based	Random Triangular (min,avg,max)	Random Triangular (min,avg,max)	None	None	Random Triangular (min,avg,max)
1 (Good driver)	95%	5%	60s,60s,90s	15s,15s,20s	15s	NA	2m,8m,20m
2 (Above average driver)	80%	20%	45s,60s,105s	10s,15s,20s	15s	NA	2m,9m,25m
3 (Average driver)	65%	35%	30s,60s,120s	5s,15s,20s	15s	NA	2m,10m,30m
4 (Below average driver)	45%	55%	15s,60s,135s	0s,10s,20s	15s	NA	2m,11m,35m
5 (Poor driver)	25%	75%	0s,60s,150s	0s,5s,15s	15s	NA	2m,12m,40m

6.5.3.2 Resource 1B: Miner crossing the gulley volatility table definition (AWS and ESS)

Various types of miners cross the gulley during operations. Activities from these miners that have a direct safety impact on the environment are discussed in this section. Probabilities are set that will influence the path followed in the workflow trees of the model when errors are introduced. When determining the probability of routes, it is important to take all interfaces involved in each activity into consideration. These

interface definitions (as defined in the functional analysis) are used to motivate parameter selections.

When the system is in the unsafe state and a miner approaches the gulley to cross, different routes can be followed as defined in Figure 28 and Figure 36 for the AWS and ESS respectively. The actions taken by the miner crossing are as follows:

Air whistle system (Option 1)

- The miner crossing signals to the driver to trip the system (correct action);
- The miner crossing uses the gulley in the unsafe state (unsafe action).

Electronic signalling system (Option 2)

- The miner crossing signals to the driver to trip the system (correct action);
- The miner crossing trips the system from the gulley (counterproductive action but safe);
- The miner crossing uses the gulley in the unsafe state (unsafe action).

Although the correct actions are indicated, it is still possible that the alternative actions are executed. The probability of executing an unsafe or counterproductive action would increase as the risk level of the miner increases. Also, the probability of executing an incorrect action is dependent on the amount of information available to the resource. Thus, if limited information is available to indicate the state of the environment (by using the signalling system's user interface in the form of buzzers and LED indicators), it is more likely that the gulley will be used in the unsafe state when compared to a system where the environment state is clearly visible. The information available indicating the environment state to the miner crossing the gulley is defined by interface 5 from Figure 26 for the AWS and in interfaces 5 and 7 from Figure 34 for the ESS.

The probabilities for actions to be followed when a miner crosses the gulley are dependent on activities 7, 8 and 11 and these probability values are shown in Table 14 (on the next page) for both systems. The AWS system has no indication of the environment state and this should be determined by analysing the gulley to determine whether the scraper winch is running. Alternatively, for the ESS, the environment state is clearly indicated by each signalling unit along the gulley by means of a bezel. Thus, given the same risk type of miner crossing the gulley, a failure is more probable for the AWS compared to the ESS for these activities.

Table 14: Miner type crossing the gulley volatility table (AWS and ESS)

Resource risk level: **Miner crossing gulley**	**Activity 11:** **Signals to the driver to trip the system**		**Activities 7 and 8:** **Trips the system from the gulley**		**Activities 7,8 and 11 altenative action:** **Uses the gulley in the unsafe state**		**Activity 11 Action:** **Signals "gulley crossed" to the driver**	**Activity 11 Alternative action:** **Fails to signal "gulley crossed" to driver**
System configuration	AWS	ESS	AWS	ESS	AWS	ESS	AWS & ESS	AWS & ESS
Deviation function	Probability Based		Probability Based		Probability Based		Probability Based	Probability Based
1 (Good miner)	90%	80%	0%	20%	10%	0%	90%	10%
2 (Above average miner)	75%	60%	0%	30%	25%	10%	75%	25%
3 (Average miner)	60%	40%	0%	40%	40%	20%	60%	40%
4 (Below average miner)	45%	20%	0%	50%	55%	30%	45%	55%
5 (Poor miner)	30%	0%	0%	60%	70%	40%	30%	70%

The probability of a failure, given a low risk resource (level 1) is set to be 10% for the AWS and 0% for the ESS. The probability of failure increases as the resource risk level increases, up to a 70% failure rate for the AWS and 40% failure rate for the ESS for a resource of risk level 5. Note that the trip function is an additional control implemented in the ESS system, and the system can be tripped directly from the gulley. This function is not possible for the AWS and therefore the probability for Activities 7 and 8 are set to 0% for the AWS.

The action where the miner crossing needs to signal that the gulley has been crossed should also be evaluated. This is part of Activity 11 (*Signal from gulley*). For some types of miners, this function might be ignored once the gulley has been crossed, with the result that the winch driver will keep on waiting for the gulley to clear (until a timeout has been reached). The volatility of this action is also shown in Table 14. Note that the probability of a failure is implemented similarly for both the AWS and ESS for this task, as there is no differentiating interface between the two systems when this task is performed.

The selection of the human risk level parameters, representing human failures and deviations for the AWS and ESS systems, to construct the volatility tables in Table 13 and Table 14 was done from logical reasoning and observations of underground operations by the research team. These are thus carefully considered values but the selection of values may differ between different teams. This error is addressed by the relativistic approach followed, as systems are directly compared. Thus, as long as the selection of the parameters is carried out in such a way that the increase or decrease in failures for the same activities is in the correct direction (given the interfaces available to the humans) it will be possible to determine feasible results during the ABR process.

6.5.4 Air whistle system (AWS) simulation model process properties

Each of the functions as presented in the generic simulation model layout (Figure 40 and Figure 41) is implemented as a process in the SIMIO environment. Each of these processes has numerous properties that can be configured, and the selection of these properties is presented in this section.

In this section, the functions from the functional flow in Figure 27 and Figure 28 are transformed to the model processes and parameters are shown for both human resources of the AWS system.

6.5.4.1 Option 1 - Winch operator (1A) model implementation

Inspect air whistle system (Option 1, 1.1A)

This function is implemented in the *InspectSystem* process. Once entered, this process has a specific processing time, after which the process will exit. The details are as follows:

```
Process: InspectSystem
Processing time: Random.Triangular(2,10,20)
Processing time units: Minutes
```

Repair fault (Option 1, 1.2A)

This function is implemented in the *RepairFault* process. This process will only be entered if a fault has been detected during the pre-shift inspection. The processing times for this fault can be from a few minutes up to a complete shift (or even days). The processing time is set to be:

```
Process: RepairFault
Processing time: Random.Triangular(0.25,1,8)
Processing time units: Hours
```

Note that the route to this function is disabled in the initial simulation where the primary focus is on the system operation. This function will be specifically investigated later in the analysis when the impact for this specific activity is evaluated.

Need to scrape ore? (Option 1, 1.3A)

This function is implemented in the *NeedToScrapeOre* process of the model. This process has a specific processing time, after which the entity (winch driver) will exit the process. The average time for a driver to determine whether ore needs to be scraped is set to 30 seconds but some deviations will be present. The deviation function is set as follows:

```
Process: NeedToScrapeOre
Processing time: Random.Triangular(1,30,60)
Processing time units: Seconds
```

Prestart (Option 1, 1.4A)

This function is represented by the *Prestart* process in the model. The prestart time for the air whistle system is not fixed as this is determined by the operator. Typically, there will be deviations for specific winch drivers. Implementation of the processing times was discussed in Section 6.5.3.1 and shown in Table 13.

Do production (Option 1, 1.5A, 1.6A, 1.7A)

The *DoProduction* process incorporates three system functions (1.5A, 1.6A and 1.7A). As the objective of the simulation is to do production, the aim of the model is for the entity (winch driver) to be in the *DoProduction* process. Therefore, the winch driver will be in this process unless production has been completed or a miner signals to the driver to cross the gulley from where the winch should be stopped. Upon these requests this process will exit.

Master stop winch (Option 1, 1.8A)

Once the scrape ore session has been completed, the winch driver should stop the winch. This is a relatively simple task and is represented by the *TripWinch* process in the model. The processing time to do this function is implemented as follows:

```
Process: TripWinch
Processing time: Random.Triangular(2,5,10)
Processing time units: Seconds
```

Signal received form gulley (Option 1, 1.9A)

This function requires the winch driver to stop the winch. When this signal is generated (by the miner crossing the gulley) the system state will be flagged and is evaluated continuously in the *Prestart* and *DoProduction* processes. The model will react accordingly and move the entity (winch driver) to the *SignalReceivedFromGulley_Unsafe* process or *SignalReceivedFromGulley_Prestrt* process. The processing times for these processes are limited as the processing time is also addressed in the model instance of the miner crossing the gulley.

Signal back to gulley (Option 1, 1.10A)

This function is implemented as part of the *MastTripWinch* process that is defined in the following point (1.11A). Note that it is possible that the driver could stop the winch first and then signal back to the gulley if required. This is not a critical function of the system as the miner crossing the gulley can also determine whether the winch has stopped if no signal has been received from the driver.

Master stop winch (Option 1, 1.11A)

This function is implemented in the *MastTripWinch* process. The processing time for this function is set to:

```
Process: MastTripWinch
Processing time: Random.Triangular(2,5,10)
Processing time units: Seconds
```

Wait for gulley crossed signal (Option 1, 1.12A)

This function is implemented in the *WaitGulleyClear* process of the model. The model entity (winch driver) will be in this process until the gulley crossed signal has been received.

A timeout is also implemented for this process if the miner crossing should fail to signal once he has completed the gulley crossover. The timeout value and deviation will depend on the type of winch driver. This function timeout has already been discussed and deviation parameters are shown in Table 13.

The remaining processes for this resource (Winch Operator) that are not defined in the section above will not be used for the modelling of the air whistle system (Option 1). The routes to these processes will be disabled when the generic model for the air whistle system is evaluated.

6.5.4.2 Option 1 – Miner crossing the gulley (1B) model implementation

Miner determines environment state before crossing the gulley (Option 1, 1.1B)

This function is represented by the *DetEnvState* process in the simulation model. The resource entity (miner crossing) will enter this process before the gulley will be entered. In this process, the current state of the environment should be determined. The average processing time for this determination is set at 15 seconds as the air whistle system option does not indicate the environment state. The state is determined by assessing the gulley to find whether the scraper winch is running. A deviation for this process is introduced by the following function:

```
Process: DetEnvState
Processing time: Random.Triangular(1,15,30)
Processing time units: Seconds
```

Once the state has been determined, the function will exit and follow the appropriate route. Note that three routes can be followed if the system is in the unsafe state. The route followed will be determined by the type of miner crossing as defined in Table 14.

Signal to driver to trip the winch (Option 1, 1.2B)

This function is represented by the *SigToDriverToTripWinch* process in the model. The processing time for this action is set to an average of 5 seconds with some deviation.

```
Process: SigToDriverToTripWinch
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Miner enters the gulley area in safe state (Option 1, 1.3B)

This function is implemented with the *MinerEnterGulleySafe* process together with the *MinerInGulleySafe* process. The time for the *MinerEnterGulleySafe* process is set to a minimum while the entity (miner crossing) will be in the *MinerInGulleySafe* process for the duration of the gulley cross time. In the *MinerInGulleySafe* process, the states of the system are evaluated continuously to determine whether the system state has changed to prestart or unsafe (initiated by the winch operator). If the system state has changed, these states will be evaluated periodically. Alternatively, this process will end once the gulley cross time has been reached. The gulley cross time is set to be an average of 30 seconds with a deviation function added as follows:

```
Process: MinerInGulleySafe
GulleyCrossTime: Random.Triangular(10,30,60)
GulleyCrossTime units: Seconds
```

Signal to driver not to start the winch (Option 1, 1.4B)

This function is implemented by the *MinerSigToDriverToTripPrestart* process in the generic simulation model. To execute this function the following time function will be set:

```
Process: MinerSigToDriverToTripPrestart
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Miner exits the gulley area in safe state (Option 1, 1.5B)

This function is represented by the *MinerExitsGulleySafe* process in the model. In this function the miner is actually still inside the gulley (hazard) and the aim of the model for the miner is to be in the *MinerInGulleySafe* process. Thus, the processing time for this function is kept to a minimum, resulting in the entity entering the *MinerExitsGulleySafe* process and exiting immediately.

(This process is not critical to the model but is added to make the simulation model a complete representation of the resource functional flow from the functional analysis).

Signal to winch operator gulley crossed (Option 1, 1.6B)

This function is implemented in the *MinerSignalsToWOGulleyCrossed* process. The process time for this function is as follows:

```
Process: MinerSignalsToWOGulleyCrossed
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Note that this function can also be bypassed if the miner crossing should fail to execute this function. This probability is added to the model according to the volatility table for the type of miner crossing (see Table 14).

Gulley crossed complete (Option 1, 1.7B)

This function is implemented in the *GulleyCrossedSafeState* process and the *GulleyCrossedUnsafeState* process. These are 'sink' processes that will remove the entity from the system. The function is split into these two processes to keep count of the miners crossing the gulley for both states. As the entities pass into these processes the *GulleyCrossedSafeCount* and *GulleyCrossedUnsafeCount* variables will be incremented accordingly to determine the number of miners that crossed the gulley in each state. These variables will be used as response measures for the model.

Miner enters the gulley area in unsafe state (Option 1, 1.8B)

This function is represented by the *MinerEnterGulleyUnsafe* process and *MinerInGulleyUnsafe* process. This function is implemented in a similar way to function 1.3B, where the time for the *MinerEnterGulleyUnsafe* process is kept to a minimum. Once entered in the unsafe state, the aim is for the entity to be in the *MinerInGulleyUnsafe* process where the state of the system is continuously evaluated. If the system state changes, the appropriate route will be followed. Alternatively, this process will end once the gulley cross time has expired. The gulley cross time implementation is explained in function 1.3B for this Option.

Signal to driver to trip the system (Option 1, 1.9B)

While the miner crossing is in the unsafe state, it is still possible for him to signal to the driver to stop the winch. This function is represented by the *SigToDriverToTripUnsafe* process. This function is implemented similar to 1.4B.

```
Process: SigToDriverToTripUnsafe
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Miner exits the gulley area unsafe (Option 1, 1.10B)

This function is represented by the *MinerExitsGulleyUnsafe* process. In this function the miner is actually still inside the gulley (hazard) and the aim of the model is for the miner to be in the *MinerInGulleyUnsafe* process. Thus, the processing time for this function is kept to a minimum, resulting in the entity entering the *MinerExitsGulleyUnsafe* process and exiting immediately.

(This process is not critical to the model but is added to make the simulation model a complete representation of the resource functional flow from the functional analysis.)

Accident occurs (Option 1, 1.11B, 1.12B, 1.13B)

The three types of accidents that can occur are evaluated in the *MinorAccident* process, *MajorAccident* process and *FatalAccident* process. These are ‘sink’ processes that will remove the entity from the system. The routes to these processes are set according to the link weights, which represent the probability of such an accident when a miner is in the gulley. The link weights are part of the input parameters of the model. When an entity (miner crossing) enters this ‘sink’ process, it will be removed from the model.

The remaining processes for this resource (Miner Crossing the Gulley) that were not defined in the section above will not be used for modelling of the air whistle system (Option 1). The routes to these processes will be disabled when the model is evaluated for the air whistle system.

The primary parameters and implementation for the model processes representing human resources were discussed in the section above for Option 1. Note that additional rules apply to the overall functional / process flows. Implementation of the overall process flows are not discussed in detail as these process flows represent the overall system operation, and are driven by the remaining resources (equipment and environment). Complete details for the process flows of the generic model implementation can be found on the accompanying compact disc (*Winch Signalling Model Contents Report V4.pdf*).

6.5.5 Electronic signalling system (ESS) simulation model process properties

The same generic model (see Figure 40 and Figure 41) is used for the implementation of the electronic signalling system in the SIMIO simulation package. Again, each function of the functional analysis (see Figure 35 and Figure 36) is modelled as a process in SIMIO with the properties of each of these processes for Option 2 (ESS) being defined in the following paragraphs. Note that the SIMIO process implementation of some resource functions is the same for similar functions implemented in Option 1 (AWS).

6.5.5.1 Option 2 - Winch operator (1A) model implementation

Inspect signalling system (Option 2, 1.1A)

This function is implemented in the *InspectSystem* process. Once entered, this process has a specific processing time, after which the process will be exited. The details are as follows:

```
Processing time: Random.Triangular(2,5,20)
Processing time units: Minutes
```

Comparison to Option 1: Since the ESS safety equipment is more feature-rich, the status of the system and corresponding slave units is displayed at the main control unit. This simplifies fault finding on the system.

Repair fault (Option 2, 1.2A)

This function is implemented in the same way as for Option 1.

```
Process: RepairFault
Processing time: Random.Triangular(0.25,1,8)
Processing time units: Hours
```

Comparison to Option 1: Option 2 allows for system feedback on the display of the main unit to show the states and faults on slave / signalling units.

Need to scrape ore? (Option 2, 1.3A)

This function is implemented in the *NeedToScrapeOre* process of the model. This process has a specific processing time, after which the entity (winch driver) will exit the process. The average time for a driver to determine whether ore needs to be scraped is reduced to 20 seconds for Option 2 as the system incorporates additional lighting down the gulley, assisting the operator with the environment state. The deviation function is set as follows:

```
Process: NeedToScrapeOre
Processing time: Random.Triangular(1,20,60)
Processing time units: Seconds
```

Comparison to Option 1: This average time is reduced from 30 seconds to 10 seconds. The deviation is still the same (1 to 60 seconds).

Initiate system prestart (Option 2, 1.4A)

This function is represented by the *Prestart* process in the model. The processing time for this function is set to 15 seconds.

```
Process: Prestart
Processing time: 15
Processing time units: Seconds
```

Comparison to Option 1: The prestart time for the electronic signalling system is fixed as this function is performed by the signalling system and not the operator. Thus no deviations will occur in this process.

Do production (Option 2, 1.5A, 1.6A, 1.7A)

The *DoProduction* process incorporates three system functions (1.5A, 1.6A and 1.7A). As the objective of the simulation is to do production, the aim of the model is for the entity (winch driver) to be in the *DoProduction* process. Therefore, the driver will be in

this process unless (i) production has been completed, (ii) a miner signals to the driver to cross the gulley, or (iii) a miner trips the system from the gulley. This process will be exited upon these requests.

Comparison to Option 1: An additional route is added where this process can be interrupted when the system is tripped from the gulley. When this function executes, the electronic system will stop the winch (remove power) forcing the system into a safe state.

Master stop winch (Option 2, 1.8A)

Once the scrape ore session has been completed, the winch driver should stop the winch. This is a relatively simple task and is represented by the *TripWinch* process in the model. The process time to do this function is implemented as follows:

```
Process: TripWinch
Processing time: Random.Triangular(2,5,10)
Processing time units: Seconds
```

Comparison to Option 1: The implementation for this function is the same for both options.

Signal received from gulley (Option 2, 1.9A)

This function requires the winch driver to stop the winch. When this signal is generated (by the miner crossing the gulley) the system state will be flagged and is evaluated continuously in the *Prestart* and *DoProduction* processes. The model will react accordingly and change the entity (winch driver) state to the *SignalReceivedFromGulley_Unsafe* process or *SignalReceivedFromGulley_Prestrt* process. The processing times for these processes are limited as the processing time is addressed in the model instance of the miner crossing the gulley.

Comparison to Option 1: This function is implemented in the same way for both options.

Signal back to gulley (Option 2, 1.10A)

This function is implemented as part of the *MastTripWinch* process that is defined in the following paragraph. Note that it is possible that the driver could stop the winch first and then signal back to the gulley if required. This is not a critical function to the system as the miner crossing the gulley can also determine whether the winch has stopped if no signal had been received from the driver.

Comparison to Option 1: The implementation is the same for both options.

Master stop winch (Option 2, 1.11A)

This function is implemented in the *MastTripWinch* process. The processing time for this option is set to:

```
Process: MastTripWinch
Processing time: Random.Triangular(2,5,10)
Processing time units: Seconds
```

Comparison to Option 1: This option is implemented similarly to Option 1. In Option 1 the winch operator would stop the winch via the switch on the winch starter unit. For Option 2 this would be done by tripping the system from the signalling system.

Wait for gulley crossed signal (Option 2, 1.12A)

This function is implemented in the *WaitGulleyClear* process of the model. The model entity (winch driver) will be in this process until the gulley crossed signal is received.

A timeout is implemented for this process if the miner crossing should fail to signal once he has completed the gulley crossover. The timeout value and deviation will depend on the risk level of the winch driver in the system. This function timeout has already been discussed and the deviation parameters are shown in Table 13.

Comparison to Option 1: The implementation is the same. The same deviation parameters are also used.

Winch tripped from the gulley (Option 2, 1.13A)

This function is represented by the *WinchTripGulley* process. Once the system has been tripped from the gulley, the winch driver will no longer be able to scrape ore and the winch will be stopped by the safety system. The processing time for this function from the winch driver point of view is limited.

Comparison to Option 1: This function is not available for Option 1

Investigate tripped condition (Option 2, 1.14A)

This function is represented by the *InvestigateTrip* process. This winch driver entity will be in this process for a given time – represented by the time taken to walk to the location where the trip was initiated along the gulley, and the system must be reset before scraping operations can proceed.

The time values for this process are implemented according to the risk level of the winch driver resource, using the volatility table as proposed in Table 13 where this task is performed in activity 13. This activity and its deviation are also discussed in this section.

Comparison to Option 1: This function is not available for Option 1

System condition reset (Option 2, 1.15A)

This function is implemented by the *ResetTrippedCondition* process. This process represents the action required by the winch operator to reset the system on the slave signalling unit from where the system trip was initiated.

The processing time for this action is set to a minimum, as this processing time is already incorporated in the *InvestigateTrip* process.

Comparison to Option 1: This function is not available for Option 1

6.5.5.2 Option 2 – Miner crossing the gulley (1B) model implementation

Miner determines environment state before crossing the gulley (Option 2, 1.1B)

This function is represented by the *DetEnvState* process in the simulation model. The entity (miner crossing) will enter this process before the gulley will be entered. In this process the current state of the environment should be determined. The average processing time for this determination is set to be five seconds as the electronic signalling system indicates this state along the gulley. A deviation is also introduced by the following function:

```
Process: DetEnvState
Processing time: Random.Triangular(1,5,10)
Processing time units: Seconds
```

Once the state has been determined, the function will exit and follow an appropriate route. Four routes can be followed when the system is in the unsafe state. The route followed will be determined by the type of miner crossing as defined in Table 14.

Comparison to Option 1: The processing time for this process is reduced for the electronic signalling system as the system state is clearly indicated by the electronic signalling system. An additional route can also be followed from this process as the system can be tripped from the gulley.

Signal to driver to trip the winch (Option 2, 1.2B)

This function is represented by the *SigToDriverToTripWinch* process in the model. The processing time for this action is set to an average of 5 seconds with some deviation.

```
Process: SigToDriverToTripWinch
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Comparison to Option 1: This process is implemented in the same way for both options.

Miner trips the system (Option 2, 1.3B)

This function is represented by the *MinerTripSystem* process. To trip the system the miner needs to pull the signal cable for at least 2 seconds. The parameters for the implementation of this process are as follows:

```
Process: MinerTripSystem
Processing time: Random.Triangular(2,2.5,3)
Processing time units: Seconds
```

Comparison to Option 1: This function is not available for Option 1.

Miner enters the gulley area in safe state (Option 2, 1.4B)

This function is implemented with the *MinerEnterGulleySafe* process together with the *MinerInGulleySafe* process. The time for the *MinerEnterGulleySafe* process is set to a minimum while the entity (miner crossing) will be in the *MinerInGulleySafe* process for the duration of the gulley cross time. In the *MinerInGulleySafe* process, the states of the system are evaluated continuously to determine whether the system state has changed to prestart or unsafe (initiated by the winch operator). If the system state has changed, these states will be evaluated periodically. Alternatively, this process will end once the gulley cross time has been reached. The gulley cross time is set to be an average of 30 seconds with a deviation function added as follows:

```
Process: MinerInGulleySafe
GulleyCrossTime: Random.Triangular(10,30,60)
GulleyCrossTime units: Seconds
```

Comparison to Option 1: This function is implemented in the same way for Option 1 and Option 2.

Signal to driver to trip prestart (Option 2, 1.5B)

This function is implemented by the *MinerSigToDriverToTripPrestart* process in the generic simulation model. To execute this function the following time function is used:

```
Process: MinerSigToDriverToTripPrestart
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Comparison to Option 1: This function is implemented in the same way for Option 1 and Option 2.

Miner trips the prestart (Option 2, 1.6B)

This function is implemented by the *MinerTripPresart* process. In this process the miner can trip the system to the safe state by pulling the signal cable for longer than 2 seconds. The time function for this process is as follows:

```
Process: MinerTripPrestart
Processing time: Random.Triangular(2,2.5,3)
Processing time units: Seconds
```

Note that if the miner should fail to trip the prestart, or fail to signal to trip the prestart, the system will enter the unsafe state. The probability of these routes followed is determined by the miner type crossing the gulley, as shown in Table 14.

Comparison to Option 1: This function is not available for Option 1.

Miner exits the gulley area in safe state (Option 2, 1.7B)

This function is represented by the *MinerExitsGulleySafe* process in the model. In this function the miner is actually still inside the gulley (hazard) and the aim of the model is for the miner to be in the *MinerInGulleySafe* process. Thus, the processing time for this function is kept to a minimum, with the result that the entity will enter the *MinerExitsGulleySafe* process and exit it immediately.

(This process is not critical to the model but is added to make the simulation model a complete representation of the resource functional flow from the functional analysis.)

Comparison to Option 1: This function is implemented in the same way for both models.

Signal to winch operator gulley crossed (Option 2, 1.8B)

This function is implemented in the *MinerSignalsToWOGulleyCrossed* process. The process time for this function is as follows:

```
Process: MinerSignalsToWOGulleyCrossed
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Note that this function can be bypassed if the miner crossing should fail to execute this function. This probability is added to the model according to the volatility table for the type of miner crossing (see Table 14).

Comparison to Option 1: This function is implemented in the same way for both system options.

Gulley crossed complete (Option 2, 1.9B)

This function is implemented in the *GulleyCrossedSafeState* process and the *GulleyCrossedUnsafeState* process. These are 'sink' processes that will remove the entity from the system. The function is split into these two processes to keep count of the miners crossing the gulley for both states. As the entities pass into these processes the *GulleyCrossedSafeCount* and *GulleyCrossedUnsafeCount* variables will be incremented accordingly to determine the number of miners that crossed the gulley in each state. These variables will be used as output measures to the model.

Comparison to Option 1: This function is implemented similar for both systems.

Miner enters the gulley area in unsafe state (Option 2, 1.10B)

This function is represented by the *MinerEnterGulleyUnsafe* process and *MinerInGulleyUnsafe* process. This function is implemented in a similar manner to function 1.4B, where the time for the *MinerEnterGulleyUnsafe* process is kept to a minimum. Once entered in the unsafe state, the aim is for the entity to be in the *MinerInGulleyUnsafe* process where the state of the system is continuously evaluated. If the system state changes, an appropriate route will be followed. Alternatively, this process will end once the gulley cross time has expired. The gulley cross time implementation is explained in function 1.4B for this option.

Comparison to Option 1: This function is implemented similar for Option 1 and 2.

Signal to driver to trip the system (Option 2, 1.11B)

While the miner crossing is in the unsafe state, it is still possible for him to signal to the driver to stop the winch. This function is represented by the *SigToDriverToTripUnsafe* process. This function is implemented similar to 1.5B.

```
Process: SigToDriverToTripUnsafe
Processing time: Random.Triangular(4,5,8)
Processing time units: Seconds
```

Comparison to Option 1: Implemented in the same way for both options.

Miner trips the system (Option 2, 1.12B)

This function is represented by the *TripUnsafe* process. This process is implemented in a similar manner to function 1.3B where the miner can trip the system when it is in the unsafe state. The parameters are as follows:

```
Process: TripUnsafe
Processing time: Random.Triangular(2,2.5,3)
Processing time units: Seconds
```

Comparison to Option 1: This function is not available for Option 1.

Miner exits the gulley area unsafe (Option 2, 1.13B)

This function is represented by the *MinerExitsGulleyUnsafe* process. In this function the miner is actually still inside the gulley (hazard) and the aim of the model is for the miner to be in the *MinerInGulleyUnsafe* process where all states are evaluated. Thus, the processing time for this function is kept to a minimum, with the result that the entity will enter the *MinerExitsGulleyUnsafe* process and exit immediately.

(This process is not critical to the model but is added to construct the simulation model as a complete representation of the resource functional flow from the functional analysis performed.)

Comparison to Option 1: This function is implemented in the same way for both options.

Accident occurs (Option 2, 1.14B, 1.15B, 1.16B)

The three types of accidents that can occur are evaluated in the *MinorAccident* process, *MajorAccident* process and *FatalAccident* process. These are 'sink' processes that will remove the entity from the system. The routes to these processes are set according to the link weights which represent the probability of such an accident when a miner is in the gulley. These link weights are part of the input parameters of the model. When an entity (miner crossing) enters this 'sink' process, it will be removed from the model.

Comparison to Option 1: No difference exists between the model options.

6.5.6 Model configuration and simulation goal (AWS and ESS)

Input parameters for both models are set in this section. The input parameters will be set to run simulations for specific scenarios using the generic simulation model. These parameters are discussed in this section in addition to the response measures used (and evaluated) in simulations. The simulation goal is also discussed, where response measures are defined for the risk-related response measures of the system used for evaluation.

6.5.6.1 Input parameters

The input parameters of the generic model are discussed as follows:

- Experiment replications
  This parameter is used to set the number of simulations that will be run for the same input parameters. Due to the model's stochastic nature, multiple

simulation runs will be executed to determine the average, minimum and maximum response values for each simulated scenario. The simulation package provides confidence intervals for these values. Thus, increasing the number of iterations improves the confidence interval of the response measures, given a specific confidence level. The confidence level is set to 95% for the simulation runs.

- Simulation run time

  The simulation run time is the production period, which is typically one shift long (8 hours). A winch driver resource (1A) will enter the system at the start of the production run and will remain there, while miners will be crossing the gulley throughout this period. This is a worst-case scenario as debarring typically takes place before the scraper and winch start running, but since the same condition holds for all systems, this has no material effect on a relativistic comparison.

- Resource 1B interarrival time

  The interarrival time of this resource (miner crossing the gulley) is defined by this parameter. A random deviation for arrival times is used in the form of a triangular function. A resource entity (resource 1B) enters the system every time this event is triggered.

  For the simulation, miners will be released into the simulation run at an average rate of one miner every 10 minutes, with the following deviation function:

  ```
  Parameter: MinerCrossingInterarrivalTime
  Parameter value: Random.Triangular(0,10,30)
  Units: Minutes
  ```

- GulleyCrossTimeTyp

  This parameter represents the time it will take to cross a gulley, allocated to the miner crossing the gulley. An average value of 30 seconds is used for crossing a gulley, with random variation around this value as some gulleys might be crossed more easily than others. This parameter is selected as follows:

  ```
  Parameter: GulleyCrossTimeTyp
  Parameter value: Random.Triangular(10,30,60)
  Units: Seconds
  ```

- WaitGulleyClearTime

  This parameter contains the time the winch driver waits for the gulley to clear once he has stopped the winch when requested (via signal) from the gulley. This parameter is set to be 60 seconds, with a deviation depending on the winch driver type. This deviation is presented by the values of activity 12 in Table 13.

- Prestart Time

  In Option 1, this parameter represents the time a winch driver takes to execute the forewarn task. The time for this task is dependent on the resource type, as discussed in Section 6.5.3.1. For Option 2, this value will be fixed as the prestart is a system function and not a resource function in the design of the ESS.

Linkweights are used to set the probabilities of a route to be followed when multiple paths exist from a node in the system. A link weight is set to each path option, representing the probability of a path being followed. When the link weight is set to 0, the path will be disabled. Link weights on paths are used to configure the volatility of human resource types as discussed in Section 6.5.3. The link weight parameters used to configure the model for this option are as follows:

- LinkWeight: MinerTripSyst

  This link weight represents the probability of a miner tripping the system from the gulley. This link weight will be set to 0 for Option 1 (AWS). This disables the route that can be followed for tripping the system as the trip function is not present for the air whistle system (Option 1).

- LinkWeight: MinerSigToTrip

  This link weight represents the probability of the miner crossing the gulley signalling to the winch driver to stop/trip the winch when in the unsafe state.

- LinkWeight: MinerFailToTrip

  This link weight is used to set the probability where the miner enters the gulley in the unsafe state, thus not signalling to the winch driver to stop the winch.

- LinkWeight: MinerSignalGulleyCrossed

  This link weight represents the probability that the miner crossing the gulley signals to the winch driver that the gulley has been crossed. This allows the winch driver to proceed with production.

- LinkWeight: MinerFailToSignalGulleyCrossed
  This link weight represents the probability that the miner crossing the gulley does not signal to the winch driver that the gulley has been crossed. This will result in the winch driver continuing to wait for the gulley to clear, until this state will eventually timeout.
- LinkWeight: WinchDriverTripWhenRequestedFromGulley
  This link weight represents the probability of the winch driver stopping / tripping the winch when requested to do so from the gulley.
- LinkWeight: WinchDriverFailToTripWhenRequestedFromGulley
  This link weight represents the probability of the winch driver not stopping / tripping the winch when requested to do so from the gulley.

6.5.6.2 Output / response measures

The following output measures will be evaluated during the model simulation:

- TotalMinersCrossingReleased
  This value represents the number of entities, miners crossing the gulley (resource 1B), that have entered the system during the simulation.
- DoProductionTime
  This value represents the time in hours that the winch driver was able to do production. Note that this value will always be less than the simulation run time.
- MinersInGulleyTime
  This value indicates the total time it took for all miners crossing the gulley during the simulation. Thus, the total processing time for all processes representing an entity in the gulley. This value includes both the safe and unsafe states of the resource in the gulley.
- MinersInGulleySafeTime
  This value represents a time percentage of the miners crossing the gulley in the safe state. This parameter will be a percentage of the *MinersInGulleyTime* parameter
- MinersInGulleyUnsafeTime
  This value represents a time percentage of the miners crossing the gulley in the unsafe state. This parameter will be the remaining percentage of the *MinersInGulleyTime* parameter.

- MinersExitGulleySafeCount
  This value represents the number of miners that exited (crossed) the gulley in the safe state (winch not running).
- MinersExitGulleyUnsafeCount
  This value represents the number of miners that exited (crossed) the gulley in the unsafe state.

6.5.6.3 Model goal (ABR Step 6)

The goal of the simulation model is to quantify the safety related risks and production related risks of each system by varying input parameters. Variations in input parameters define specific scenarios that will be simulated in experiments. The selection of the risk response parameters, as required from ABR step 6, is presented in this section.

Risk-related measures for production:

The risk relating to production is translated to production time loss from the model. This is done by evaluating *DoProductionTime* output parameter against the *SimulationTime* input parameter. When the exposure to production loss is a minimum, the *DoProductionTime* needs to be a maximum.

Risk-related measures for safety:

The risk relating to safety is translated to hazardous exposure time and occurrences of hazardous instances in the model. This representation indicates the time (expressed as a percentage) that humans are in the gulley in an unsafe state. These hazardous exposure times can further be translated to minor, major or fatal accidents, given historic data. Hazardous exposure is the combined *MinersInGulleyUnsafeTime* and *MinersInGulleySafeTime* output measures. For the hazardous exposure to be a minimum, *MinersInGulleyUnsafeTime* needs to be a minimum. These parameters will be expressed as a percentage of the total time a miner is in the gulley. When expressing this as a percentage, the parameter value is not directly dependent on the number of miners crossing the model. If the number of miners crossing the gulley increases / decreases, this value will not be significantly affected, given the remaining input parameters remain the same for the scenario – but this will have an impact on the production-related risk. The variables *MinersExitGulleySafeCount* and *MinersExitGulleyUnsafeCount* parameters could also have been used, but these values only represent the state when the miner was exiting the gulley. The time parameters take into account instances where a miner

could have entered the gulley in the safe state, but exited during the unsafe state (and vice versa).

The aim of the model would be to find the system where the hazardous exposure time and the production time loss is at an acceptable level. The generic simulation model allows the determination of these risks. As this is a relativistic study, the associated risks for each system can be determined and compared for each scenario.

In the end, the candidate system that gives the best balance between a low hazardous exposure time and a high production time will be the winning system. The safety equipment used in this system will be selected as the equipment to be acquired, and will also give the set of requirements to be used in the mine's acquisition process. Also, since the simulations were done using real-world, integrated scenarios, the mine will understand the interaction of the TO-BE technology with humans in the system and will be empowered to make informed decisions on support, such as training, employment of new personnel, and so on.

6.5.6.4 Experiments

Experiments will be set up to represent each concept model (AWS and ESS). Unique input parameters can be defined for each model and experiment. Scenarios are defined for all experiments for which to compare output measures. Experiments will include variation of risk levels of human resources in the system.

Each system option (AWS and ESS) consists of two human resources (winch driver and miner crossing the gulley). As five resource risk levels have been identified, 25 combinations of scenarios exist that must be considered in analyses.

In this case study, experiment 1 is set to be the default experiment of each system. In this experiment, all system (equipment) functions are set to the default states as it should be in operations. This experiment consists of 25 scenarios where the human resource combinations differ between scenarios. The results are evaluated using this experiment from each concept design to determine the results for ABR step 7. Thereafter experiments 2 to 15 are performed, each representing a specific activity failure or deviation. Each of these experiments is run with 25 scenarios representing the combination of human resource types introduced into the model. These experiments are required to perform the activity-based risk analysis of the system, as presented in Step 8 of the ABR process.

6.5.7 Simulation results for AWS and ESS (ABR Step7)

In this section, simulation results for the air whistle system and electronic signalling system are evaluated. In the first two sub-sections, these options are evaluated individually, after which they are directly compared to determine the risk contribution in terms of production time loss and hazardous exposure for each system.

6.5.7.1 Simulation results (Option1, Experiment1)

This section shows the simulation results for the model configured for Option 1 (AWS). Experiment 1 is the default experiment where all activities are set to be “normal” as defined in the functional analysis of the air whistle system (AWS), with the input parameters as defined in Sections 6.5.4 and 6.5.6.1. The complete set of input parameters, in the form of a summary table, can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*).

The results for the 25 scenarios of Option 1 (AWS) are shown in Table 15. The experiment was run for 8-hour operational shifts with 200 simulation runs to provide results with a 95% confidence level.

Table 15 (on the next page) shows the output measures as averages for all simulation runs. Each scenario is defined by the winch driver risk level (WDLevel) and a miner crossing the gulley risk level (MCLevel). The results clearly indicate that human resource actors influence the model outputs significantly. The outputs shown in the table are the average number of miners crossing the gulley during a simulation run (1), the number of these miners that have exited (crossed) the gulley in the safe (2) and unsafe (3) states, the time that miners were in the gulley in the unsafe state (4), expressed as a percentage of the total time miners were in the gulley. These values will be used to determine the hazardous exposure time of the system. The average production time (5) is also shown. This parameter shows the time production was done, expressed as a percentage of the total simulation (8 hours). This parameter is used to represent the production time loss for a specific scenario.

Table 15: Option 1, Experiment 1 results

Option 1: Experiment 1 ("Normal")							
Scenario number	Scenarios	Experiment Replications	Avg: Total Miners Crossing Released	Avg: Miner Exit Gulley Safe Count	Avg: Miner Exit Gulley Unsafe Count	Avg: Miners In Gulley Unsafe Time	Avg: Do Production Time
1	Air Whistle Op1 WDLevel1, MCLevel1	200	36.5	32.8	3.6	10%	91%
2	Air Whistle Op1 WDLevel1, MCLevel2	200	36.5	27.5	8.9	25%	91%
3	Air Whistle Op1 WDLevel1, MCLevel3	200	36.4	22.1	14.2	39%	92%
4	Air Whistle Op1 WDLevel1, MCLevel4	200	36.5	17.3	19.2	53%	93%
5	Air Whistle Op1 WDLevel1, MCLevel5	200	36.3	12	24.3	67%	95%
6	Air Whistle Op1 WDLevel2, MCLevel1	200	36.9	32.4	4.4	12%	91%
7	Air Whistle Op1 WDLevel2, MCLevel2	200	36.8	26.4	10.3	28%	92%
8	Air Whistle Op1 WDLevel2, MCLevel3	200	36.5	20.9	15.4	42%	93%
9	Air Whistle Op1 WDLevel2, MCLevel4	200	36.4	15.4	20.9	58%	94%
10	Air Whistle Op1 WDLevel2, MCLevel5	200	36.7	10.3	26.3	72%	95%
11	Air Whistle Op1 WDLevel3, MCLevel1	200	36.5	31.3	5.1	13%	92%
12	Air Whistle Op1 WDLevel3, MCLevel2	200	36.8	24.3	12.4	34%	93%
13	Air Whistle Op1 WDLevel3, MCLevel3	200	36.6	18.9	17.6	48%	94%
14	Air Whistle Op1 WDLevel3, MCLevel4	200	36.5	13.4	23	63%	95%
15	Air Whistle Op1 WDLevel3, MCLevel5	200	36.6	8.8	27.7	76%	96%
16	Air Whistle Op1 WDLevel4, MCLevel1	200	36.6	25.9	10.5	22%	92%
17	Air Whistle Op1 WDLevel4, MCLevel2	200	36.6	19.1	17.4	43%	94%
18	Air Whistle Op1 WDLevel4, MCLevel3	200	36.4	13.9	22.4	58%	95%
19	Air Whistle Op1 WDLevel4, MCLevel4	200	36.8	9.4	27.3	72%	96%
20	Air Whistle Op1 WDLevel4, MCLevel5	200	36.9	6.6	30.3	81%	97%
21	Air Whistle Op1 WDLevel5, MCLevel1	200	36.4	14.6	21.6	45%	94%
22	Air Whistle Op1 WDLevel5, MCLevel2	200	36.6	9.5	26.9	65%	95%
23	Air Whistle Op1 WDLevel5, MCLevel3	200	36.3	6.6	29.7	76%	96%
24	Air Whistle Op1 WDLevel5, MCLevel4	200	36.7	4.4	32.2	84%	97%
25	Air Whistle Op1 WDLevel5, MCLevel5	200	36.8	3.3	33.5	89%	97%

The output results for the *DoProductionTime* and *MinersInGulleyUnsafeTime* response parameters can be illustrated in the form of a SMORE chart by SIMIO. This is an enhanced version of a Nelson's MORE chart. The black bar shows the complete range of observations while the rectangular box shows the region containing observations between lower (25%) and upper (75%) percentile points. The confidence interval on the mean is represented by the tan-coloured box, while the confidence intervals of the upper and lower percentile points are represented by the light blue boxes [71]. The SMORE plots of the output responses for Option1, experiment1 are shown in Figure 42 and Figure 43 respectively.

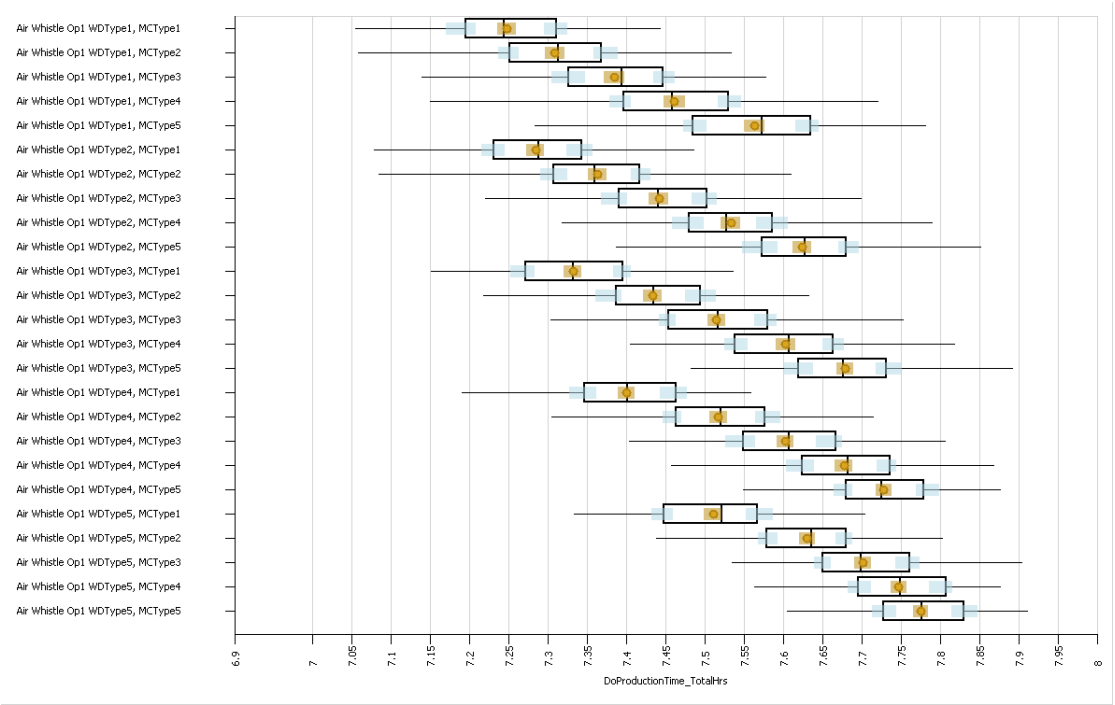


Figure 42: Option1, experiment 1 *DoProductionTime* output response

The SMORE chart in Figure 42 represents the population range for the *DoProductionTime* response of the air whistle system (Option 1). Each scenario represents a combination of the human resource risk levels used in the system. These scenarios are represented by the SMORE chart for 200 simulation runs. The confidence levels are also shown (light blue and tan-coloured boxes). As the number of observations increases (by increasing the number of simulation runs), the confidence intervals decrease.

The chart from Figure 42 indicates that the production performed using the air whistle system as a safety measure will actually increase with an increase in the risk levels of the human resources used. It is also seen that the selected output evaluation parameters (in terms of production and safety) are more sensitive towards the risk levels of miners crossing the gulley, than to the risk level of the winch operator.

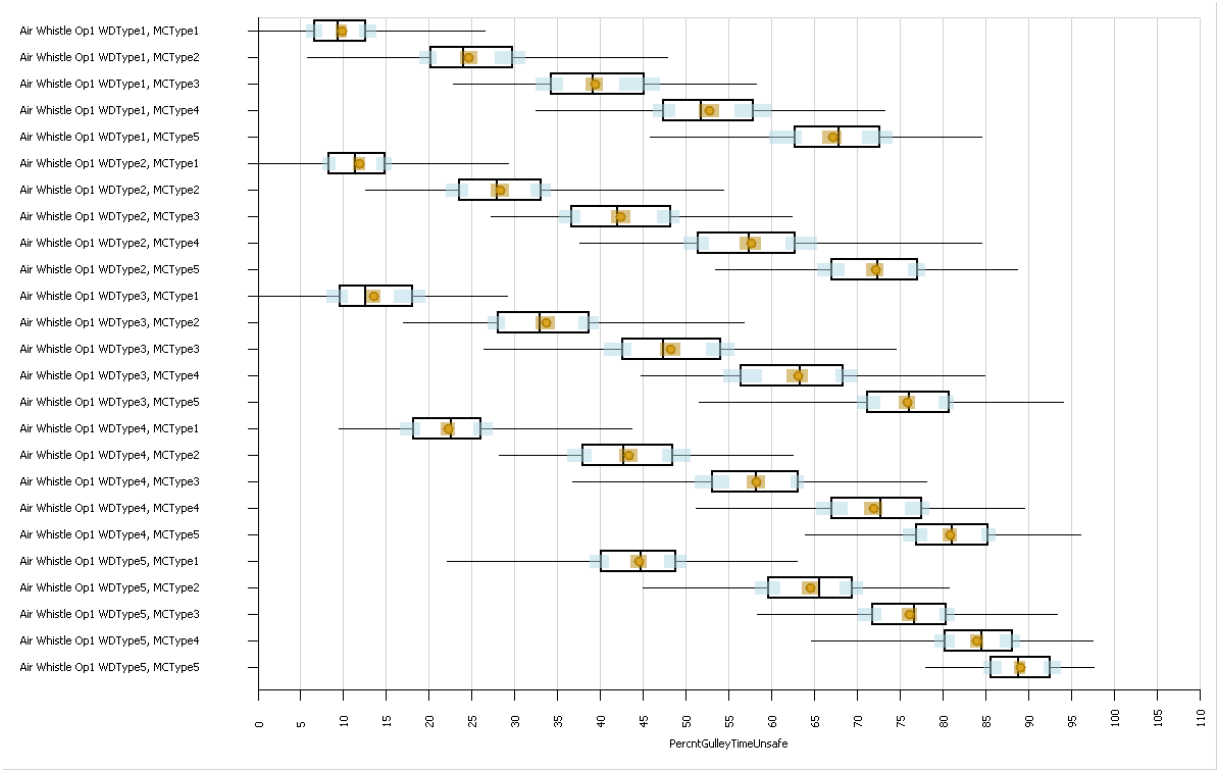


Figure 43: Option1, experiment 1 *GulleyTimeUnsafe* output response

Figure 43 illustrates a SMORE chart using the *GulleyTimeUnsafe* as a response. Note that this variable indicates the percentage of the time that the miners crossing the gulley were in the unsafe state. By evaluating these values one can determine the time humans are exposed to hazardous operations in a simulation. It is clear that system safety is affected more by a deviation in the risk level of the miner crossing the gulley than for a deviation in the risk level of the winch driver operating the winch. The results also show that, as the risk levels of the resources using the system increase, the safety of operations is significantly compromised.

Evaluating the air whistle system, the simulation shows that even with low risk resources, the system's hazardous exposure time is fairly high. The scenario with the lowest mean hazardous exposure time is still 11%, while the maximum hazardous exposure time for this system is at 88%. The average hazardous exposure time for the 25 identified scenarios is at 49%. This indicates that when an average risk level operator and winch driver are used, almost half of the time when the miner would cross the gulley, he would be in the unsafe state. As this unsafe state increases, the probability of an accident increases.

Production time seems to be fairly high for this system. Even when the production time is at its lowest, it is still 87% of the maximum possible production time.

Given the simulation results of the air whistle system, the production output (time) is definitely acceptable, although it is observed that this system does not provide sufficient safety to address winch-related accidents as hazardous exposures time are shown to be significantly high.

The values generated from the simulation runs are dependent on the input parameters and assumptions made in the implementation of the simulation, as discussed. Although these outputs do not necessarily represent the exact real world implementations and bias may be present, it is important that the same parameters and assumptions be used when comparing different systems. Thus the focus will be on the differences evaluated in the responses of the system outputs when the systems are compared. Keeping this in mind, the simulation results for the electronic signalling system are evaluated in the following section.

6.5.7.2 Simulation results (Option2, Experiment 1)

This section evaluates the simulation results for the configured model of the electronic signalling system (Option 2). The same experiment will be run as for the air whistle system (Option 1) of the previous section. During this experiment, all activities are set to be “normal” as defined in the functional analysis of this electronic signalling system. These parameters are defined in Sections 6.5.5 and 6.5.6.1. The complete set of input parameters, in the form of a summary table can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*).

The output results for the 25 scenarios of Option 2 are shown in Table 16. The experiment used 200 simulations runs to give a confidence level of 95%, as with Option 1. It was important to keep the number of iterations the same for both options, as the results from Option 1 and Option 2 will be compared to determine the risk-related factors in each system.

Table 16: Option 2, Experiment 1 results

Option 2: Experiment 1 ("Normal")							
Scenario number	Scenarios	Experiment Replications	Avg: Total Miners Crossing Released	Avg: Miner Exit Gulley Safe Count	Avg: Miner Exit Gulley Unsafe Count	Avg: Miners In Gulley Unsafe Time	Avg: Do Production Time
1	Electronic Signalling Op2 WDLevel1, MCLevel1	200	36.4	36.4	0.0	0%	78%
2	Electronic Signalling Op2 WDLevel1, MCLevel2	200	36.9	33.7	3.1	9%	73%
3	Electronic Signalling Op2 WDLevel1, MCLevel3	200	37.0	30.9	6.0	17%	67%
4	Electronic Signalling Op2 WDLevel1, MCLevel4	200	36.7	27.6	9.1	25%	65%
5	Electronic Signalling Op2 WDLevel1, MCLevel5	200	36.9	25.4	11.5	31%	61%
6	Electronic Signalling Op2 WDLevel2, MCLevel1	200	36.4	36.4	0	0%	74%
7	Electronic Signalling Op2 WDLevel2, MCLevel2	200	36.4	32.9	3.4	10%	68%
8	Electronic Signalling Op2 WDLevel2, MCLevel3	200	36.8	30.5	6.2	18%	64%
9	Electronic Signalling Op2 WDLevel2, MCLevel4	200	36.8	27.8	8.9	25%	60%
10	Electronic Signalling Op2 WDLevel2, MCLevel5	200	36.9	26.1	10.7	29%	57%
11	Electronic Signalling Op2 WDLevel3, MCLevel1	200	37.0	36.9	0.0	0%	69%
12	Electronic Signalling Op2 WDLevel3, MCLevel2	200	36.7	33.3	3.4	9%	63%
13	Electronic Signalling Op2 WDLevel3, MCLevel3	200	36.9	30.7	6.2	17%	59%
14	Electronic Signalling Op2 WDLevel3, MCLevel4	200	36.9	28.4	8.6	24%	56%
15	Electronic Signalling Op2 WDLevel3, MCLevel5	200	36.9	26.7	10.2	28%	53%
16	Electronic Signalling Op2 WDLevel4, MCLevel1	200	36.6	36.4	0.2	0%	61%
17	Electronic Signalling Op2 WDLevel4, MCLevel2	200	36.5	32.7	3.8	11%	56%
18	Electronic Signalling Op2 WDLevel4, MCLevel3	200	36.7	30.2	6.4	18%	53%
19	Electronic Signalling Op2 WDLevel4, MCLevel4	200	36.9	28.5	8.4	23%	51%
20	Electronic Signalling Op2 WDLevel4, MCLevel5	200	37.0	27.2	9.8	26%	50%
21	Electronic Signalling Op2 WDLevel5, MCLevel1	200	36.5	35.2	1.2	1%	47%
22	Electronic Signalling Op2 WDLevel5, MCLevel2	200	36.6	32.4	4.2	11%	46%
23	Electronic Signalling Op2 WDLevel5, MCLevel3	200	36.3	29.5	6.8	19%	48%
24	Electronic Signalling Op2 WDLevel5, MCLevel4	200	36.7	28.8	7.8	21%	47%
25	Electronic Signalling Op2 WDLevel5, MCLevel5	200	36.9	27.6	9.2	25%	48%

Table 16 shows the averages of output measures for all simulation runs, similar to the table in Option 1. Each scenario is defined by the winch driver risk level (WDLevel) and the miner crossing the gulley risk level (MCLevel). The results clearly indicate that these human resource factors influence the response measures significantly. The outputs shown in the table are the average number of miners

crossing the gulley during a simulation run (1), the number of these miners that have exited (crossed) the gulley in the safe (2) and unsafe (3) states, and also the time that miners were in the gulley in the unsafe state (4), expressed as a percentage of the total time miners were in the gulley. These values will be used to determine the hazardous exposure time of the system. The average production time (5) is also shown. This parameter shows the time production was done, expressed as a percentage of the total simulation time.

The output results for the *DoProductionTime* and *MinersInGulleyUnsafeTime* response parameters are illustrated by the SMORE charts in Figure 44 and Figure 45.

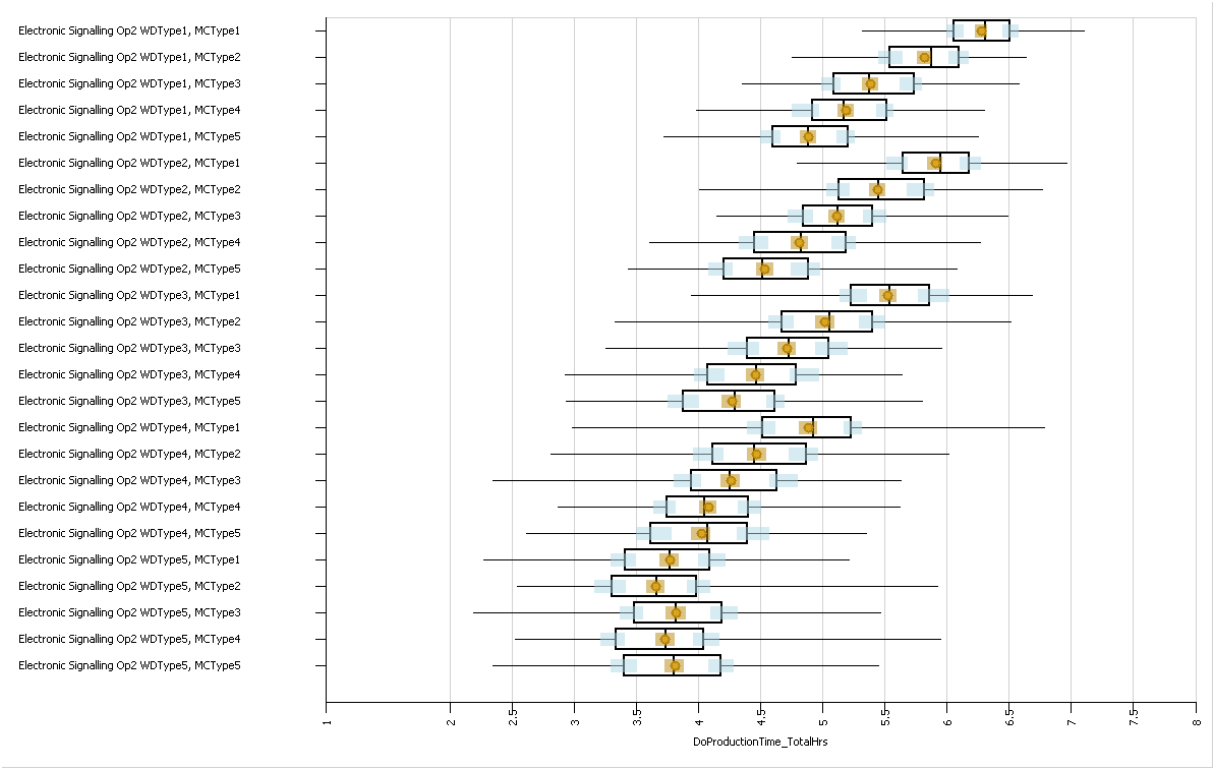


Figure 44: Option2, experiment 1 *DoProductionTime* output response

The *DoProductionTime* response output is shown in Figure 44. The human resource risk levels used are shown on the left axis, with the results for each risk level as a time value. This time value represents the time production could have been performed in an 8-hour shift. The confidence intervals are also shown (light blue and tan-coloured boxes) for each scenario.

The SMORE chart in Figure 44 indicates that the production output using the electronic safety system is fairly low. The average production time, taking all risk

levels of human resources into account, is 4.6 hours which translates to 58% of the total operation time. The maximum production time occurs when resource types WDLevel1 and MCLevel1 are used, but this output is still at 76% (mean value) of the operation time. The minimum output occurs (mean value = 47%) when the WDLevel5 and MCLevel5 resource combination is introduced into the system.

The chart in Figure 44 also indicates sensitivity with respect to resource types used for the electronic signalling system. When the winch drivers of risk levels 1 – 3 are used, the system is quite sensitive to the risk type of miners crossing the gulley. When the WDLevel4 and WDLevel5 are used, the effect of a miner risk level is reduced.

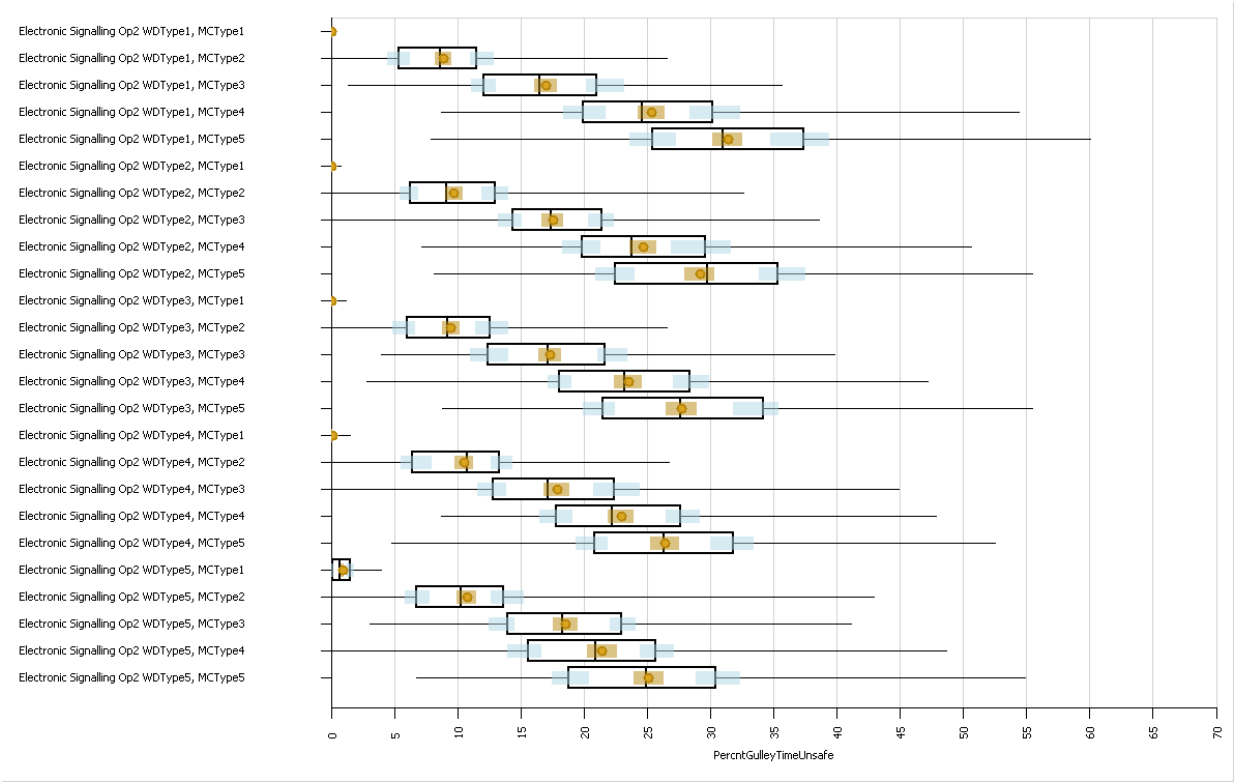


Figure 45: Option2, experiment 1 *GulleyTimeUnsafe* output response

Figure 45 shows the outputs (response measures) for the *GulleyTimeUnsafe* parameter, indicating the percentage of time that miners were in the gulley in the unsafe state. The safety risk related to hazardous exposure time when using the electronic signalling system is addressed compared to the air whistle system. The average hazardous exposure time for the electronic signalling, given all scenarios identified, is at approximately 16%. The maximum hazardous exposure time occurs when the MCLevel 5 resource is used (mean value = 30%). The minimum hazardous exposure time occurs when the MCLevel1 is involved, as the time value is at 0% for these scenarios.

The sensitivity of hazardous exposure time with respect to the resource risk score for the electronic signalling system is also indicated by the SMORE chart in Figure 45. The sensitivity with respect to the winch driver risk score appears to be limited, while the system is more sensitive with respect to the miner crossing the gulley.

The evaluation of the electronic signalling system shows that the hazardous exposure time is reduced when compared to the air whistle system (AWS), but production time has also reduced using the electronic signalling system (ESS). Thus, the production loss exposure increases using an electronic signalling system. The two systems will be directly compared in the following section.

6.5.7.3 Results comparison: Option1 vs Option 2

In this section, results of the two options will be compared to show a relativistic comparison of production time loss and hazardous exposure time.

To compare the two options directly, normalized risk-related factors are defined (not risk in the strict definition, but rather a normalised score that fits the ontology of the mining environment). The *DoProductionTime* and *GulleyTimeUnsafe* parameters are used to determine hazardous exposure time and production time loss. These parameters will be translated into a Production Loss Factor (**PLF**) and a Hazardous Exposure Factor (**HEF**) as follows:

Production loss factor (**PLF**): The *DoProductionTime* parameter is transformed to show a percentage of total possible production time. This is done to provide a value that is directly comparable to HEF, which represents hazardous exposure time as a percentage.

As production time increases, PLF decreases proportionally. Thus, PLF is defined as follows:

$$PLF = \left(1 - \frac{DoProductionTime}{OperationsTime}\right) \cdot 10$$

The *OperationTime* is the simulation time (a shift of 8 hours) for all simulations. PLF falls on a scale of 1 – 10, thus higher values indicate higher production time loss. For example, if the PLF value is 3, it means that 30% of production time will be lost.

Hazardous exposure factor (**HEF**): The *GulleyTimeUnsafe* parameter is transformed to give HEF as the percentage value during which the gulley was used in an unsafe state. The value of HEF is given as:

$$HEF = GulleyTimeUnsafe \cdot 10$$

Thus, as the time increases for which a miner is in an unsafe gulley, the HEF increases proportionally on a scale of 1 - 10. For example, if the HEF value is 2, it means that for 20% of the time a miner is in an unsafe gulley.

The risk-related factors defined above are shown in Table 17, where both systems are compared. The factors for each option are shown, together with the factor difference in the last two columns. These factors are generated from experiment 1 as discussed in the previous two sections.

Table 17: Experiment 1 risk-related factors comparison (Option1 vs Option 2)

Option1 vs Option 2: Experiment 1 ("Normal")							
		AWS (Option 1)		**ESS (Option 2)**		**Difference**	
Scenario number	**Scenarios**	**HEF** (= Miners In Gulley Unsafe Time)	**PLF** (1 – Do production Time)	**HEF** (= Miners In Gulley Unsafe Time)	**PLF** (1 – Do Production Time)	**HEF difference** (Op 2 – Op 1)	**PLF difference** (Op 2 – Op 1)
1	WDRL1, MCRL1	1.0	0.9	0.0	2.2	-1.0	1.2
2	WDRL1, MCRL2	2.5	0.9	0.9	2.7	-1.6	1.9
3	WDRL1, MCRL3	3.9	0.8	1.7	3.3	-2.2	2.5
4	WDRL1, MCRL4	5.3	0.7	2.5	3.5	-2.7	2.8
5	WDRL1, MCRL5	6.7	0.5	3.1	3.9	-3.6	3.3
6	WDRL2, MCRL1	1.2	0.9	0.0	2.6	-1.2	1.7
7	WDRL2, MCRL2	2.8	0.8	1.0	3.2	-1.9	2.4
8	WDRL2, MCRL3	4.2	0.7	1.8	3.6	-2.5	2.9
9	WDRL2, MCRL4	5.8	0.6	2.5	4.0	-3.3	3.4
10	WDRL2, MCRL5	7.2	0.5	2.9	4.3	-4.3	3.9
11	WDRL3, MCRL1	1.3	0.8	0.0	3.1	-1.3	2.3
12	WDRL3, MCRL2	3.4	0.7	0.9	3.7	-2.4	3.0
13	WDRL3, MCRL3	4.8	0.6	1.7	4.1	-3.1	3.5
14	WDRL3, MCRL4	6.3	0.5	2.4	4.4	-4.0	3.9
15	WDRL3, MCRL5	7.6	0.4	2.8	4.7	-4.8	4.3
16	WDRL4, MCRL1	2.2	0.8	0.0	3.9	-2.2	3.1
17	WDRL4, MCRL2	4.3	0.6	1.1	4.4	-3.3	3.8
18	WDRL4, MCRL3	5.8	0.5	1.8	4.7	-4.0	4.2
19	WDRL4, MCRL4	7.2	0.4	2.3	4.9	-4.9	4.5
20	WDRL4, MCRL5	8.1	0.3	2.6	5.0	-5.4	4.6
21	WDRL5, MCRL1	4.5	0.6	0.1	5.3	-4.4	4.7
22	WDRL5, MCRL2	6.5	0.5	1.1	5.4	-5.4	5.0
23	WDRL5, MCRL3	7.6	0.4	1.9	5.2	-5.8	4.9
24	WDRL5, MCRL4	8.4	0.3	2.1	5.3	-6.3	5.0
25	WDRL5, MCRL5	8.9	0.3	2.5	5.2	-6.4	5.0
	Avg:	**5.1**	**0.6**	**1.6**	**4.1**	**-3.5**	**3.5**

Table 17 shows the HEF and PLF as differences between Option 2 (ESS) and Option 1 (AWS). Green values show where the related risk-related factors decreased using the ESS while red values show an increase when using the ESS. It is clear from this comparison that the production loss increases significantly using the ESS while the hazardous exposure decreases significantly when using the ESS.

The graphs generated in Figure 46 and Figure 47 compare the PLF and HEF respectively for both systems. Note that the graph presented is sorted according to the human resource risk levels / scores.

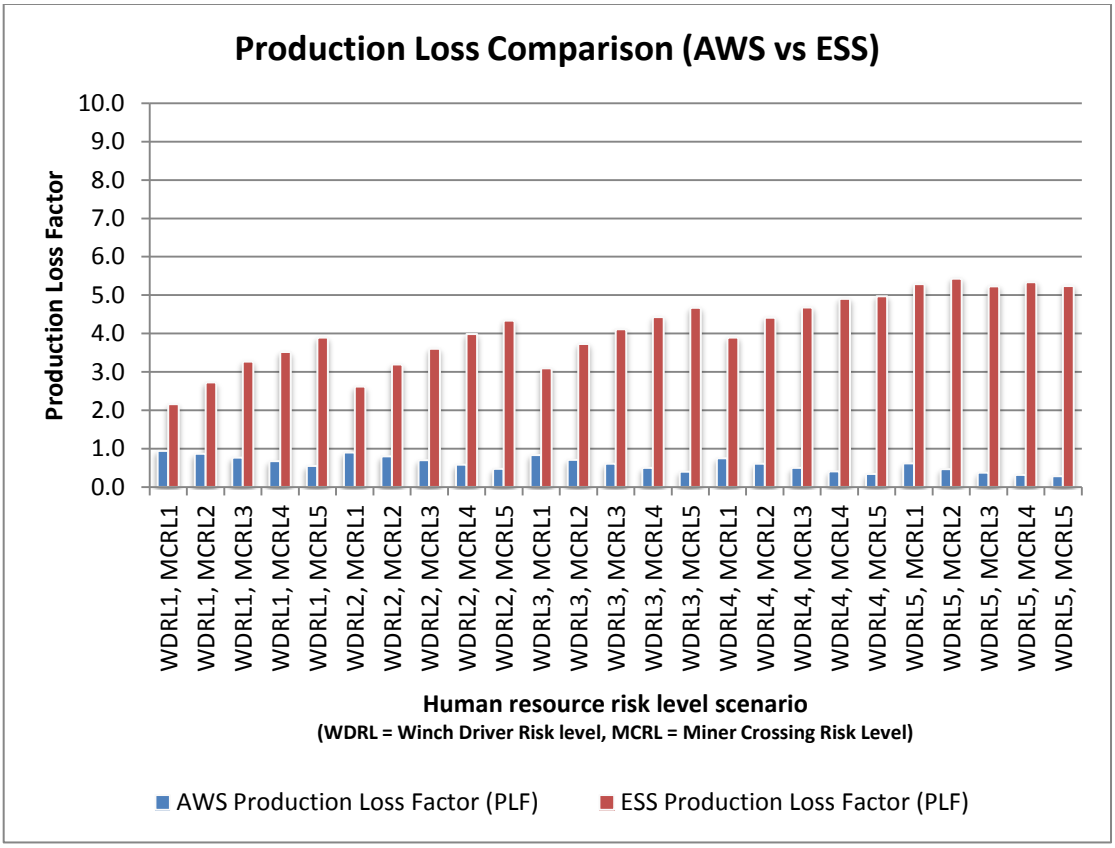


Figure 46: PLF comparison (AWS and ESS)

Figure 46 shows the PLF comparison for the two options. It is clear that, for the air whistle system (AWS), the PLF is a minimum. In the worst case scenario the PLS is less than 1.5 for the AWS. One also observes that the PLF increases as the risk level of the human resources decreases. This is because, as the winch driver risk level increases, the more a winch driver will ignore signals from the gulley, thus using the system in the unsafe state. The same happens with the miners crossing, as their risk level increases, the more will they ignore (or fail to determine) the gulley state and cross the gulley in the unsafe state.

The production loss for the electronic signalling system (ESS) is significantly higher than for the AWS. Even in the best case scenario (WDRL1, MCRL1), the PLF for the

ESS is still at 2.4. As the PLF increases from one scenario to another for the AWS, it decreases for the ESS. This is mostly because the ESS is a more complex system, where more deviations can be introduced when a high risk level resource is used, resulting in increased production loss. This phenomenon will be further analysed in Section 6.5.8.

From the analysis above, it is observed that the AWS is more sensitive for a risk level change in the miner crossing the gulley than for a risk level change in the type of winch operator used. In the ESS, the PLF of the system is fairly sensitive for the miner crossing the gulley risk level 1 – 5 and the winch driver risk level is from 1 – 3. With the winch driver risk level being 4 and 5, the system is less sensitive for the type of miner crossing the gulley. These sensitivities are also determined (and more visible) in the SMORE charts of Figure 42 and Figure 44.

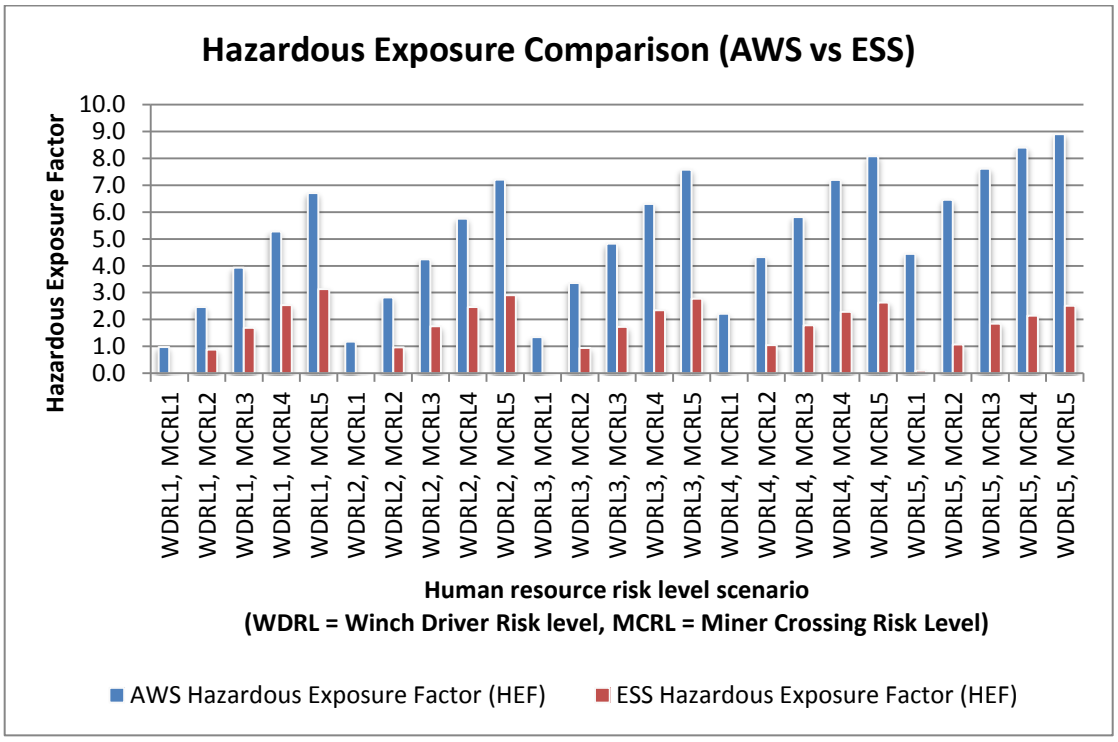


Figure 47: HEF comparison (AWS and ESS)

The HEFs of the AWS and ESS systems are compared in Figure 47. It is clear from the figure that the HEF for the AWS is higher than the HEF for the ESS. The HEF for the AWS is also more affected, and thus more sensitive, to a change in the resource risk level (scenario). Where the difference between the minimum HEF and maximum HEF for the AWS is 7,7, it is reduced to 2,8 for the ESS.

The HEF is a minimum for both systems when the lowest risk level winch driver and miner crossing the gulley are used, as expected (WDRL1 and MCRL1). A similar trend is evident for the HEF in the ESS as for the AWS. In both systems, it appears

as if that the system is more sensitive to the risk level of the miner crossing the gulley resource than for the winch operator resource. These sensitivities are also illustrated in the SMORE charts in Figure 43 and Figure 45.

Taking the compared results for both systems into consideration, it is clear that the ESS shows a lower hazardous exposure but an increased production loss, while the opposite is true for the AWS. The system must be further analysed to determine the HEF and PLF of each activity individually. By doing this, the activities required for the determination of an enhanced system where the activities contributing to high production loss and hazardous exposure can be addressed or mitigated. This activity-based risk analysis is performed in the following section.

6.5.8 Further analysis – Activity-based risk (ABR Step 8)

In this section, both the air whistle system (AWS) and electronic signalling system (ESS) are further analysed to isolate sensitive activities with respect to hazardous exposure and production loss.

General system tasks (activities) were defined in Table 11 and Table 12 where the resource allocation was carried out in the functional analysis. All resource functions and states relevant to each activity are mapped in these tables, with the primary resources indicated (highlighted). These activities for both systems are as follows:

- Activity 1: Do pre-shift inspection
- Activity 2: Identify whether ore should be scraped
- Activity 3: Determine environment state
- Activity 4: Do prestart
- Activity 5: Trip prestart from master
- Activity 6: Trip winch from master
- Activity 7: Trip prestart from gulley
- Activity 8: Trip winch from gulley
- Activity 9: Start the winch
- Activity 10: Scrape ore
- Activity 11: Signal from gulley
- Activity 12: Wait for gulley to clear
- Activity 13: Investigate trip
- Activity 14: Reset system

Below, activity-based risk is used to determine the effects of deviations on the risk-related factors by using the simulation model from Section 6.5.

Consequently, the simulation model will be altered to incorporate adjustments to the above model as new information comes to light – this will have an effect on resources states and functions and demonstrate the value of ABR in the acquisition process.

A new experiment is set up for each activity, after which the simulation results indicate the change in that activity in terms of HEF and the PLF for the total system.

After the high risk activities have been identified (based on the output measures from the simulation model), this information is used to optimise the system to address high risk activities.

6.5.8.1 Activity 1 - Do pre-shift inspection

Activity description:

In this activity, the winch operator will inspect the signalling system to ensure the system is operational. In the case where the system is not fully functional, the system should be repaired before operations can proceed.

Primary resources:

The primary resources directly involved in this activity are the winch driver together with the signalling system itself. These same resources are required for both systems. In the case where the system is faulty, maintenance personnel will be involved.

Activity deviation experiments:

Experiments 2 and 3 (min and max)

In the generalized SIMIO model, a process is implemented representing this activity as it is one of the functions performed by the winch driver. The random processing time function for this process is set to *Random.Triangular(2,10,20)* for the AWS and *Random.Triangular(2,5,20)* for the ESS – defined in *minutes*. In the AWS, the average time is slightly longer as ESS has an additional system status indication, assisting the winch driver with the status of the system.

To determine the impact of this activity, experiment 2 will be run where the processing time for the *InspectSystemTime* is set to a fixed value of 2 minutes. Thereafter experiment 3 will be run where this input parameter will be set to a maximum of 20 minutes.

Note that this activity is not a complex task of the system with minimal inputs and outputs, the deviation in this task for the first two experiments will have a small, proportional impact on production time. Thus, if this activity were to take 20 minutes longer, production time will be 20 minutes less. As this task is implemented in the same way in both systems, the deviation impact on this task will be the same for both systems. These are obvious observations, but the experiments will still be done for the sake of showing consistency of the model. In the activities further analysed during the ABR process, where the same principle applies, the simulations will not be done explicitly as the concept has been shown in experiments 2 and 3.

Activity failure (Experiment 4)

In the scenario where the winch driver fails to report a faulty system and proceeds with operations, this will have a major impact. This impact will be evaluated in experiment 4 where the model will be reconfigured to simulate this scenario. This implementation will be different for the two signalling system options as the AWS is not integrated with the winch starter circuit, thus the winch operator can start the winch independent of the state of the AWS. In the case of the ESS, the winch cannot be started by the operator unless the ESS is in the unsafe state.

The model implementation to simulate this failure in the AWS is achieved by disabling the route where the winch driver trips the system when requested from the gulley as the winch driver will not receive this communication if the system is faulty. The winch driver would still be able to proceed with operations as normal as the AWS does not prevent him from starting the winch and scraping ore.

In the case of the ESS, this failure is addressed through a fail to safe configuration. As power to the winch is controlled by the ESS, the winch cannot operate unless the ESS allows power to the winch, which is in the system's unsafe state. When the system is faulty, the system will trip and enter the safe state once prestart is complete. This is implemented by reconfiguring the simulation model by adding a route from the output of the *Prestart* process to the input of the *NeedToScrapeOre* process. This route is forced.

The results for experiments 2, 3 and 4 are compared with the results from experiment 1 for each system option. Simulations were run for 200 iterations. The risk-related factors (HEF and PLF) for experiments 2 to 4 are shown in Figure 48 to Figure 50. These figures show the differences in risk-related measures after the results from experiment 1 (representing "normal operations") have been subtracted from the results of this experiment. More detailed simulation results for these experiments can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*).

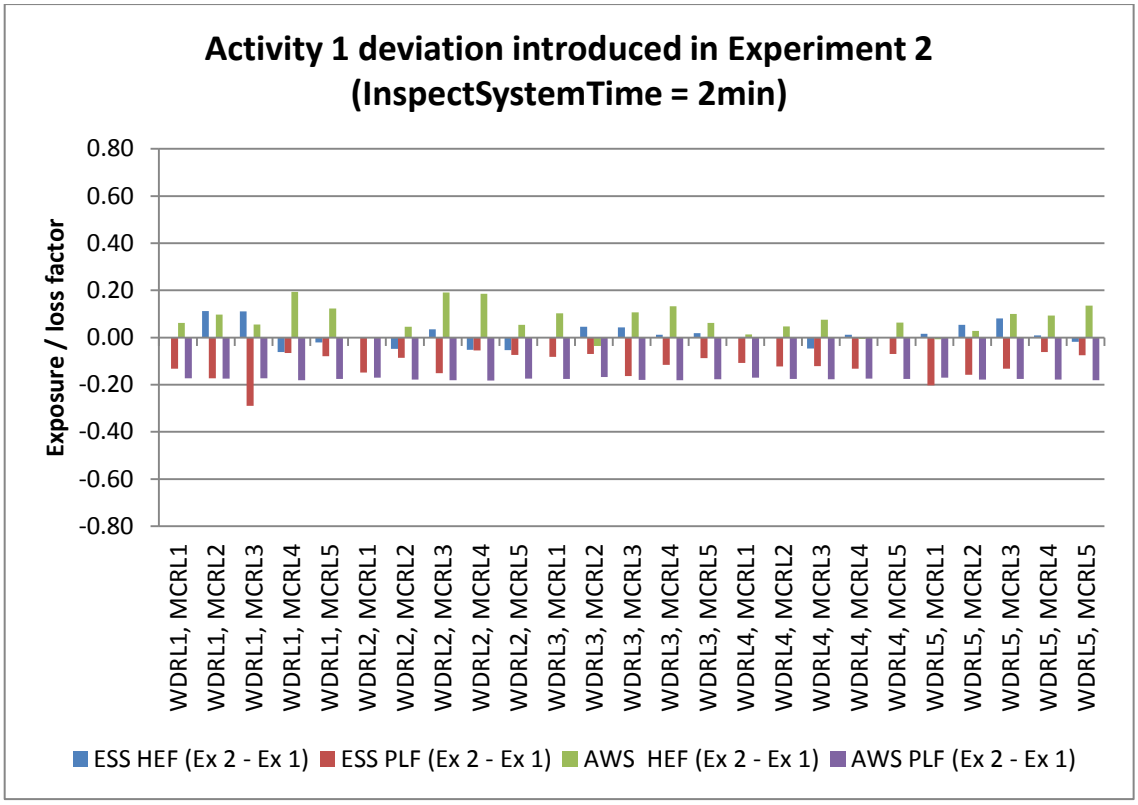


Figure 48: Activity 1 deviation introduced in Experiment 2

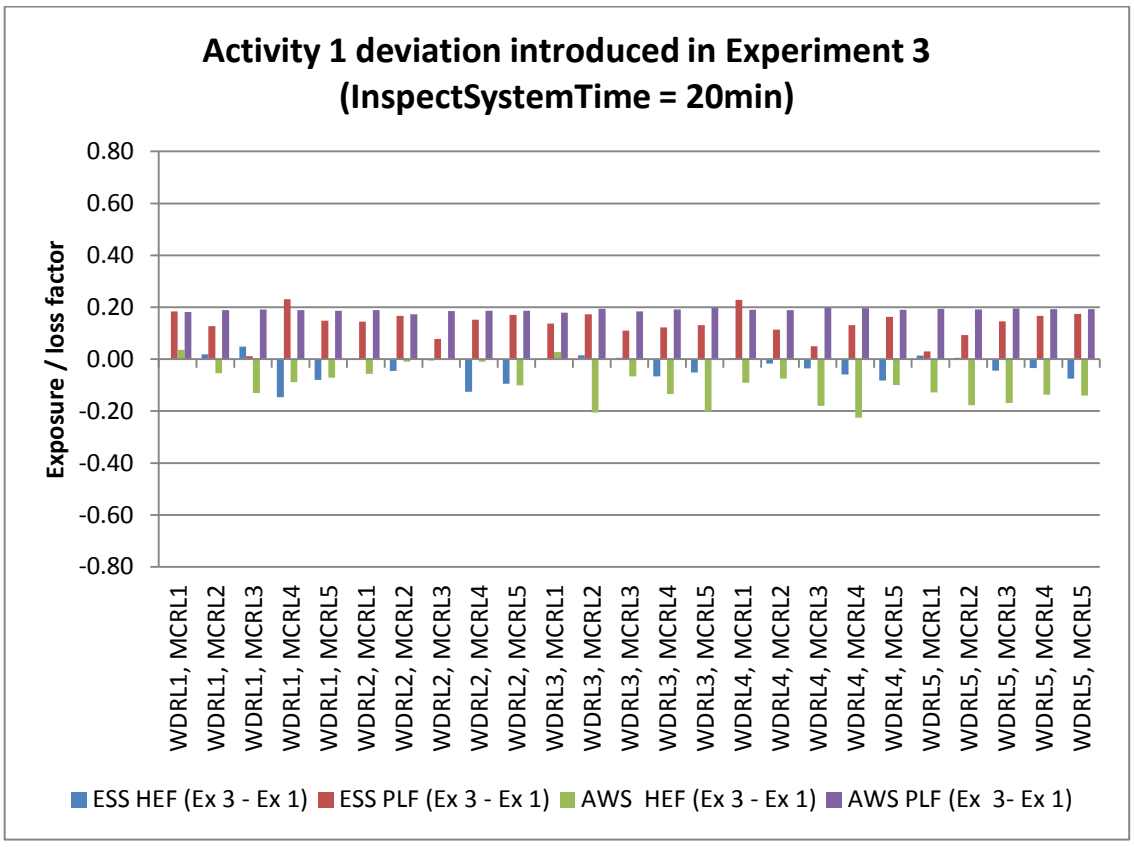


Figure 49: Activity 1 deviation introduced in Experiment 3

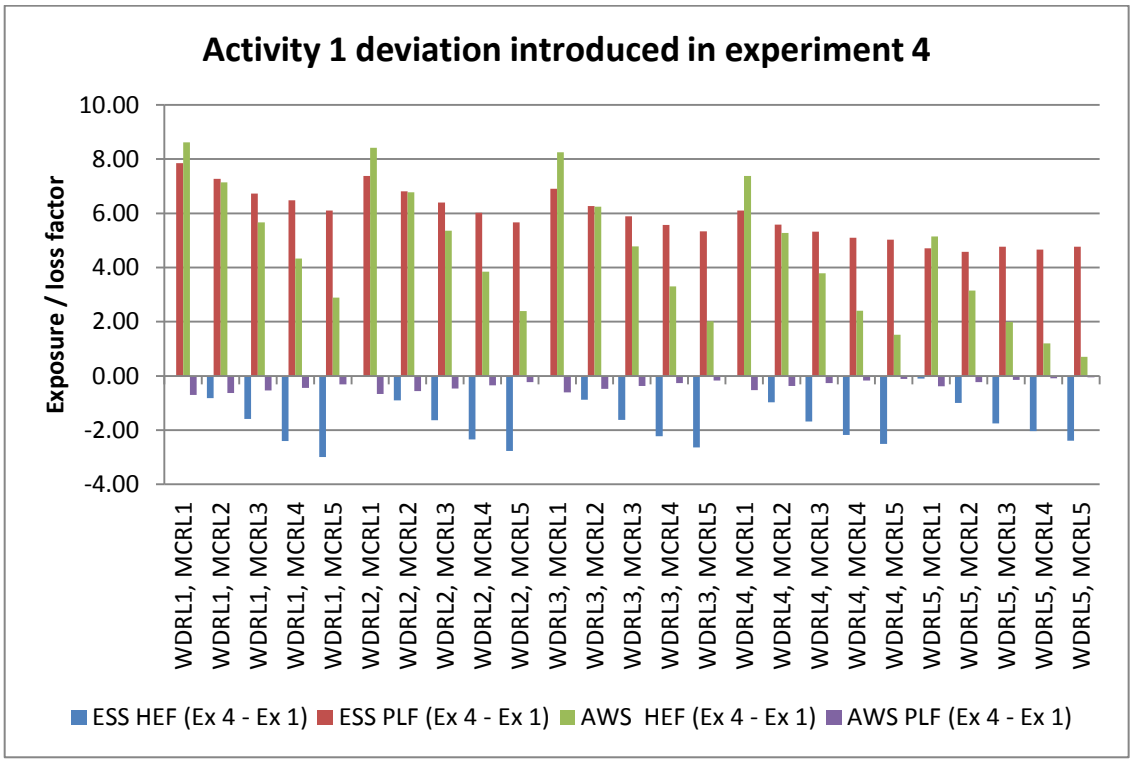


Figure 50: Activity 1 deviation introduced in Experiment 4

The results from experiments 2 and 3 show that a time deviation in this activity has limited impact when compared to the system in experiment 1, which represents "normal" operations. For both systems, the deviation in terms of the HEF and the PLF is less than 0.2. This experiments also shows, as expected, that as the time to perform this activity increases by a specific time, less production will be done by the same amount. Thus, the production loss effect is directly proportional to the delay introduced in this activity.

Experiment 4 shows a high impact in both the HEF and PLF for both systems. The results indicate that, for the AWS, the HEF is a maximum (above 9.5) while the PLF is a minimum (less than 0.3). This can be expected when the AWS is faulty and operation proceeds with this faulty system.

In the case of a faulty ESS (Experiment 4), the experimental results show that the HEF is minimum (0) while the PLF is maximum (10). This is expected as the ESS fails to safe upon a system failure, and production can no longer be performed.

The figures above show the difference in HEF and PLF when compared to the "normal operation" (experiment 1). Taking the averages of the HEF and PLF over all types of operator combinations, the effects of each experiment on this activity are summarised in Table 18 on the next page.

Table 18: Activity 1 deviation analysis summary

Activity 1	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF (Change)	AWS PLF (Change)	ESS HEF (Change)	ESS PLF (Change)
Experiment 2	Minimizing Activity Time	Yes	<0.2	<0.2	<0.2	<0.2
Experiment 3	Maximizing Activity Time	Yes	<0.2	<0.2	<0.2	<0.2
Experiment 4	Activity failure (operations proceed while system faulty)	Yes	4.6	0.5	-1.5	5.8

Observations from the table are shown below:

- A time deviation in this activity has a limited impact on both systems;
- A failure of this activity has maximum impact on the hazardous exposure of the AWS and the production loss of the ESS.

6.5.8.2 Activity 2 - Identify whether ore should be scraped

Activity description:

In this activity, the winch operator will inspect the environment and determine whether ore should be scraped. The effect on risk-related factors for this activity will be determined by implementing deviations into this process.

Primary resources:

The primary resources involved for this activity are the winch operator and the environment. The winch operator should inspect the environment (gulley) to determine whether ore needs to be scraped.

Activity deviation experiments:

Experiments 5 and 6 (min and max)

The process representing this activity in the simulation model is the *NeedToScrapeOre* process. The random processing time function for this process is set to *Random.Triangular(1,30,60)* for the AWS and *Random.Triangular(1,20,60)* for the ESS – both in *seconds*. In the AWS, the average time is slightly longer than the ESS as the ESS has additional lighting on the slave units along the gulley. This illumination assists the winch driver in determining the status of the gulley.

To determine the sensitivity of this activity the *NeedToScrapeOre* processing time is minimized (=1 sec) in experiment 5 and maximized (=60 sec) in experiment 6.

Similar to the *InspectSystem* process as shown in Experiments 2 and 3, a deviation introduced into this process has a directly proportional effect on the production time of the system. The results from experiments 5 and 6 show limited effect on risk-related factors for this deviation. This results are thus not explicitly shown for this experiment as they are similar to the results generated in experiment 2 and 3.

Activity failure experiment

This experiment introduces a failure in determination of the environment state. Two possible scenarios exist for a failure: (1) the winch operator proceeds with operations to scrape ore whilst there is no ore to be scraped, and (2) the winch operator does not proceed with operations while there is ore to be scraped.

The impact for these scenarios will be as follows:

(1) Hazardous exposure will increase as unnecessary “unsafe” operations are performed when not required;
(2) Production time loss will increase, as production is not done when required.

Activity 2 requires the winch driver to interface with the environment and is executed in a similar fashion for both signalling systems. Because this activity does not involve a direct interface with either the AWS or ESS, it will not be specifically evaluated in terms of a simulation model as the aim is to determine high risk functions in terms of the signalling system in order to optimize the equipment of the system.

The impact will be the same on both systems as this activity is dependent mainly on the winch driver. Note that in the case where hazardous exposure is increased, the ESS system will absorb more of this hazardous exposure as it is shown that the overall HEF of this system is lower than for the AWS system.

This experiment does not influence the outcome of the overall analysis in terms of optimisation of the system.

A summary of the impact for this activity is shown in Table 19 on the following page.

Table 19: Activity 2 deviation analysis summary

Activity 2	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
Experiment 5	Minimizing Activity Time	No	<0.2	<0.2	<0.2	<0.2
Experiment 6	Maximizing Activity Time	No	<0.2	<0.2	<0.2	<0.2
No specific experiment	Activity failure 1: (operations proceed while no ore is present)	No	Fair	None	Limited	None
	Activity failure 2: (operations do not proceed while ore is present)	No	None	Fair	None	Fair

Observations for the experiment are listed below:

- A time deviation in this activity has limited impact on both systems;
- A failure of this activity could add additional risk to the system, but this is similar for both systems as this activity is not specifically addressed by the signalling system (signalling system is not a primary resource).

6.5.8.3 Activity 3 - Determine environment state

Activity description:

This activity is performed by the miner who wants to cross the centre gulley. Before crossing the gulley, the miner should determine the state of the gulley and act accordingly using the signalling system.

Primary resources:

The primary resources involved in this activity are the miner crossing the gulley, the signalling system (AWS and ESS) and the environment. The miner crossing should inspect the environment to determine whether the environment is in the safe (winch not running) or unsafe (winch scraping) states. When the AWS is used, this state is not indicated. With the ESS, this state is indicated by the ESS along the gulley on the slave units (see Figure 32 and Figure 33).

Activity deviation experiments:

Time deviation (min and max)

The process representing this activity in the simulation model is the *DetEnvState* process. The random processing time function for this process is set to *Random.Triangular(1,15,30)* for AWS and *Random.Triangular(1,5,10)* for ESS – both in *seconds*. The average time of this process is longer for the AWS as the ESS indicates the environment state along the gulley.

This process has no direct impact on production of the system as production will proceed while the miner is determining the state of the gulley. A time variance in this process will also have no effect on the hazardous exposure as this process is performed before the miner enters the gulley. Thus, a time deviation in this activity will have no direct impact on the hazardous exposure or production loss of the system.

Activity failure (Experiment 7)

A failure can occur in this activity when the state of the environment is not correctly determined. For both systems, the possible states are safe, unsafe or prestart. If the system state is assessed to be safe while the system is in the unsafe or prestart state, hazardous exposure will be introduced.

This activity relates directly to the risk level of the miner crossing the gulley. This has been discussed in Section 6.5.3, where probabilities of these resource risk types were implemented in the generalized model.

Because this deviation has already been implemented in the model representing normal operations (Experiment 1), the risk-related factors for this activity will be determined when compared to the ideal scenario. To make this comparison, a scenario with an ideal winch driver and a miner crossing (both risk level 1) will be used as input parameters to represent the “optimal” resource risk level scenario. This scenario will be compared to scenarios where the other four risk levels of miners crossing the gulley are used. This simulation setup will indicate the effect of each risk type of miner crossing the gulley.

This data is available from experiment 1, and will be used to show the variations of risk levels of the miner crossing the gulley.

The results when failures are introduced for this activity are shown in Figure 51 and Figure 52 on the following page.

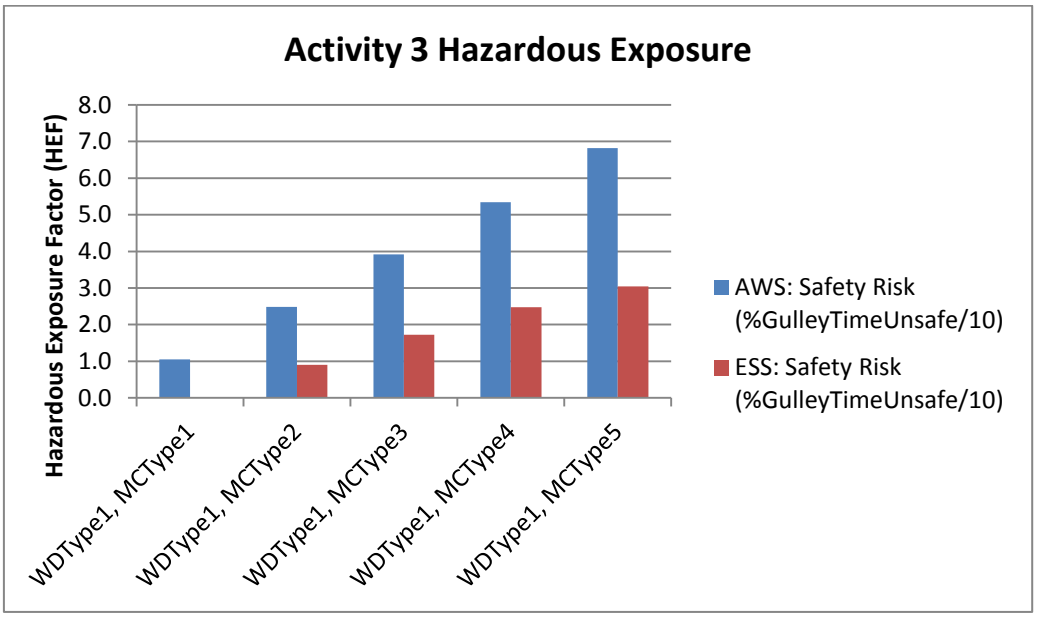


Figure 51: Activity 3 HEF comparison

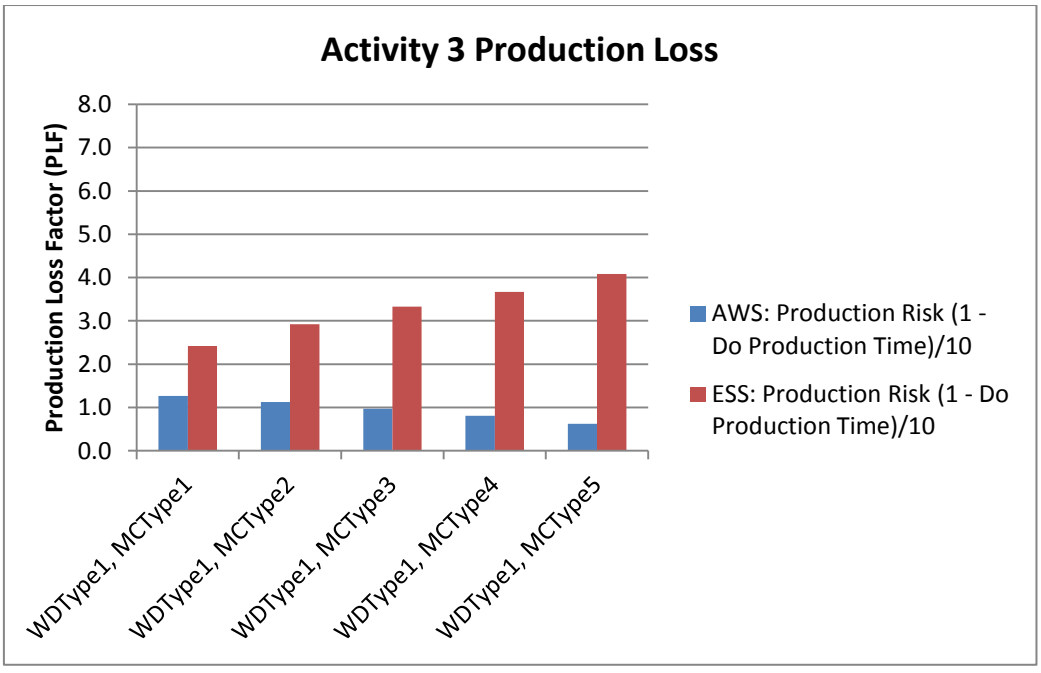


Figure 52: Activity 3 PLF comparison.

The figures above show HEF and PLF comparisons when risk levels of miners crossing the gulley are introduced. These can further be compared to the best-case scenario where both resources are at risk level 1.

The HEF for both systems increases as the risk level of the miner crossing the gulley increases. Note that the impact is more significant for the AWS, compared to the ESS.

The PLF is also affected by this activity failure. Production loss decreases for the AWS while it increases for the ESS as the miner crossing risk level increases.

A summary of the impact for this activity is shown in Table 20. The risk-related factor values for experiment 7 have been normalised to show additional risk introduced into the system by the use of higher risk resource types.

Table 20: Activity 3 deviation analysis summary

Activity 3 (Det Env state)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Experiment	Minimizing Activity Time	Yes	0	0	0	0
No experiment	Maximizing Activity Time	Yes	0	0	0	0
Experiment 7	MCRL 1	Yes	NA	NA	NA	NA
	MCRL 2	Yes	1.4	-0.1	0.9	0.5
	MCRL 3	Yes	2.9	-0.3	1.7	0.9
	MCRL 4	Yes	4.3	-0.5	2.5	1.3
	MCRL 5	Yes	5.8	-0.6	3.0	1.7

Observations from this experiment are listed below:

- The AWS safety is more sensitive with respect to a deviation in this activity, while the production loss decreases slightly;
- The ESS system is less sensitive than the AWS in terms of hazardous exposure but a production loss is introduced.

6.5.8.4 Activity 4 – Do Prestart

Activity description:

This activity is a *transitional activity* performed by the winch driver before starting the winch. For the AWS, the prestart routine requires the winch driver to swing the scraper winch cables along the gulley to indicate this state. This action is not forced from the AWS itself, and the winch can be started by the winch driver regardless of whether the prestart has been performed.

In the ESS, this function is performed by the signalling system equipment. The prestart button can be pushed when the system is in the safe state. The ESS will enter the prestart routine for a fixed time (15 seconds), during which the system

buzzer sounds and red bezels flash along the gulley. Once the prestart routine has been completed, the system enters the unsafe state and switches power through to the winch.

Primary resources:

The primary resources involved for this activity are the winch driver, the miner crossing the gulley, and the signalling system. The winch driver initiates the prestart, upon which the miner crossing should react. In the case of the ESS, this prestart task is performed by the equipment, but still initiated by the winch driver.

Activity deviation experiment:

As mentioned, the time for this activity is fixed for the ESS (as the prestart is performed by the equipment) while the time for this activity is variable for the AWS where this activity is performed by the winch driver.

In the AWS, the prestart processing time can be defined as a random variable following a triangular distribution. This deviation is the risk driver level in the general model (experiment 1) and varies from *Random.Triangular(0,5,15)* for risk level 5 to *Random.Triangular(15,15,20)* for risk level 1, where 15 seconds is the desired prestart time.

The first experiment for this activity is where the HEF and PLF deviations are determined when the prestart time is set to 0 seconds. This simulates an AWS system scenario where no prestart is executed. This is experiment 8, and will be simulated using 200 runs. The input parameters and output measures for this experiment, as implemented in the SIMIO generic model can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*).

The results for this experiment (*PrestartTime = 0 seconds*) are graphically represented in Figure 53 on the following page.

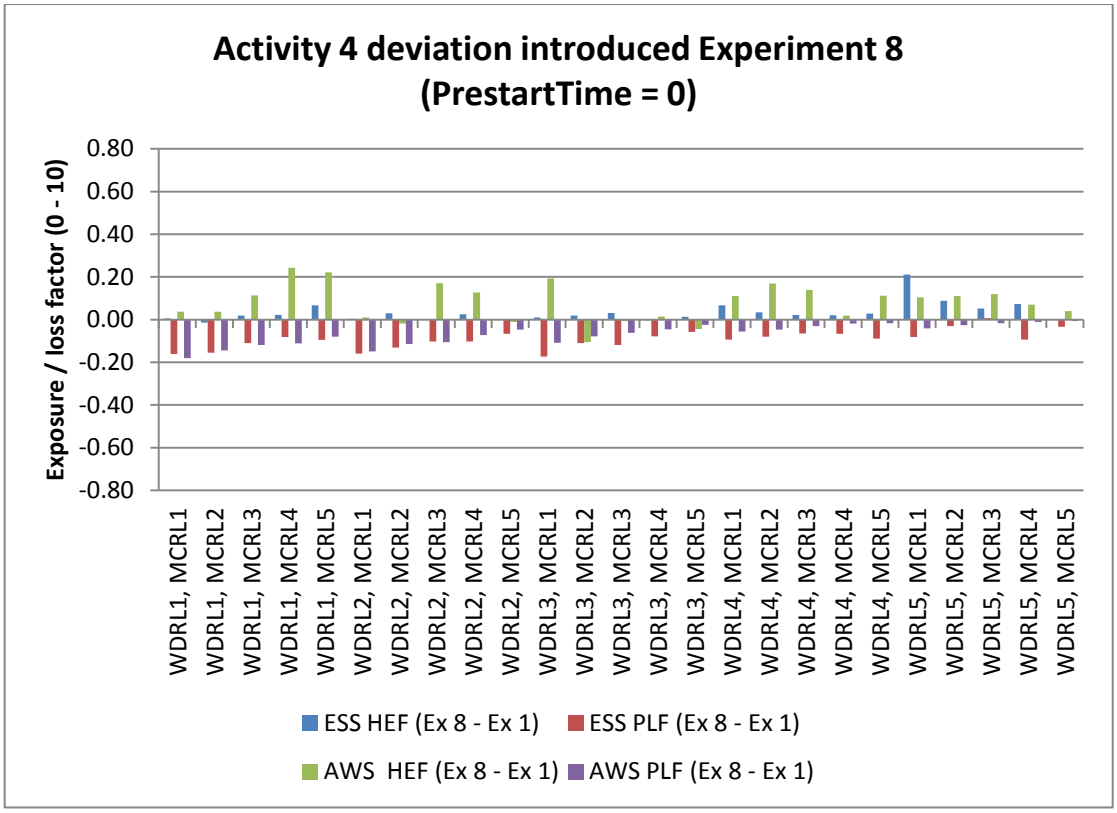


Figure 53: Activity 4 deviation introduced in Experiment 8 (PrestartTime = 0)

The results from experiment 8 show risk-related factor differences when the prestart time is set to 0 (i.e. equivalent to the prestart activity being disabled). This figure shows the difference between results from experiment 8 as compared to results from experiment 1 (normal conditions).

It is clear that the HEF increases slightly for both systems while the PLF decreases slightly.

The decrease in production loss when no prestart is available is due to the time that was allocated to the prestart function and will now be allocated to the *DoProduction* process. The prestart time (average 15 seconds) is minimal with respect to the simulation run (8 hours) so this impact is minimal for the ESS. (Note that the exposure / loss factor on the vertical axis of Figure 53 is a rating out of 10.)

When evaluating the prestart function, the absence of a prestart has limited impact on the HEF safety factor, but since the prestart activity is a transitional activity, the prestart activity could have a significant safety impact on the system, even though it is not represented in the HEF value. This is thus an example of a transitional activity between safe and unsafe states that is particularly important to analyse as comprehensively as possible.

In the scenario where no prestart is present and the winch is started, no reaction time would be allowed for the miner crossing to act. Alternatively, if the miner is in the gulley in a safe state, and a prestart routine has been executed first, the miner has been warned and could take evasive action. Thus, although the additional time represented in the HEF of Figure 53 is minimal, this unsafe time is critical and should be further investigated.

To add more weight to the hazardous exposure of an absent prestart activity, the number of occurrences in the simulation run, when the winch was started with the miner crossing being in the gulley, have to be counted. This is done by adding an additional risk response parameter, called the *WinchStartedCountWithMinersInGulley*. This value will be compared and expressed as a percentage of the number of miners released in the model to cross the gulley. We will call this the Prestart related Hazardous Exposure Factor (PHEF) as a specific instance of a transitional activity:

$$\boldsymbol{PHEF} = \frac{WinchStartedCountWithMinersInGulley}{TotalMinersReleased} \times 100$$

Thus, if the PHEF is 2, this means 2 out of a 100 miners crossing the gulley will be inside the gulley when the winch is started (this does not guarantee an accident, but the likelihood is high).

The SIMIO model is updated to determine the Prestart Risk value. This risk value is determined for experiment 1 and experiment 8 by running each experiment for 200 replications, using the updated model. Figure 54 (on the next page) shows the results when the two experiments are compared.

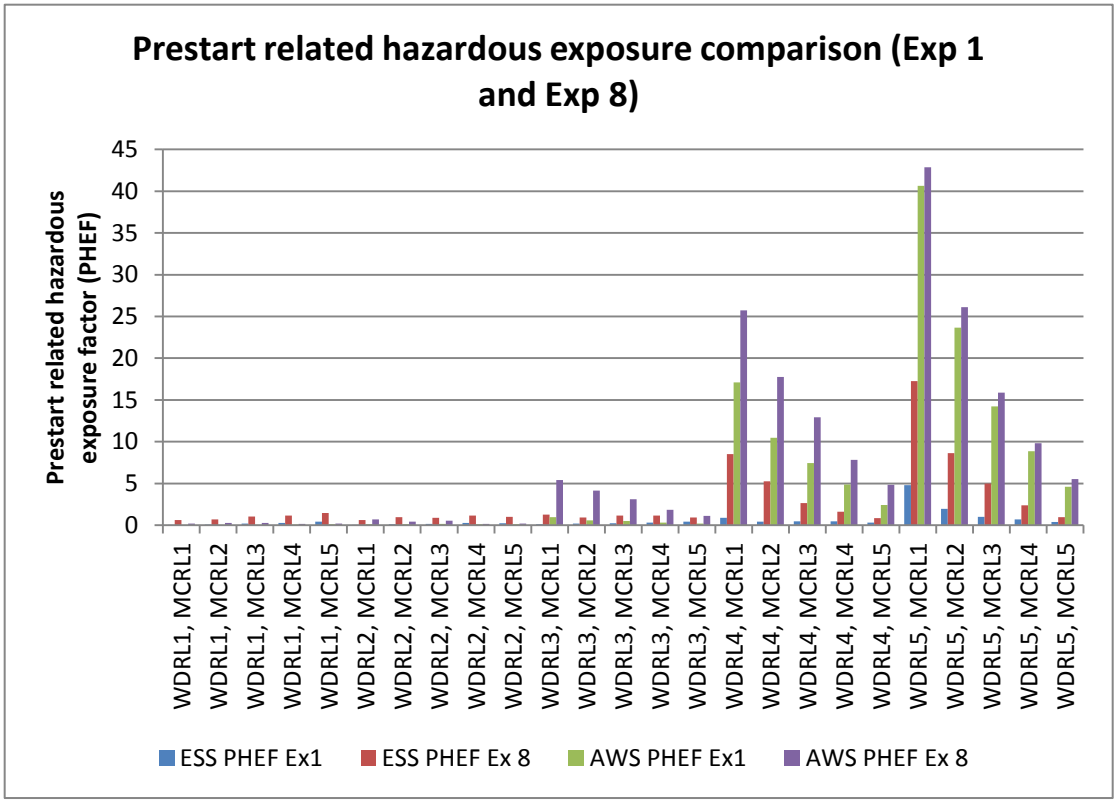


Figure 54: Prestart-related hazardous exposure comparison for Experiment 1 (normal) and Experiment 8 (Prestart = 0)

The prestart-related hazardous exposure factor is shown in Figure 54 for both systems, with and without the prestart routine. It is clear from these results that the prestart function has limited effect when winch drivers of risk level 1 and 2 are used. When a winch driver with a higher risk level is used (3, 4 and 5), the prestart hazardous exposure increases significantly for experiment 8 (no prestart) when compared to experiment 1 (with prestart). The results also show the importance of the prestart transitional activity (a function enforced by equipment). For the ESS system, where a deterministic prestart function of a fixed time can be implemented, the prestart exposure is limited throughout all winch operator and miner crossing scenarios. When the prestart function is removed from the ESS system (Experiment 8), prestart risk becomes evident, but this risk factor is still half of the risk factor of the AWS with the prestart function included (Experiment 1). When the prestart function is removed from the AWS (Experiment 8) the prestart risk value increases significantly.

Further investigation into the model was required to determine why the PHEF first starts to show once a winch driver of risk level 3 is involved in the system. The SIMIO model was run in a stepped visual mode to determine this cause. This simulation process showed the cause to be due to the *WaitGulleyClear* process. In this process, an additional time delay is allowed after the prestart, after which the winch driver

proceeds with operations if a signal has not been received when the system has been tripped (or requested to have been tripped). This timeout value is an attribute of the winch driver type in the model – the exact input parameters for this experiment can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*). The time it takes for the miner to cross the gulley is typically set to 30 seconds (with deviation), while the minimum value on the *WaitGulleyClearTime* parameter is set to be 30 seconds for winch driver type 3. This minimum value decreases as the risk rating of the winch driver type increases. This means that when winch drivers type 1 and 2 are used, they will wait long enough for the typical miner to cross the gulley before they proceed with operations again, therefore there will typically be no more miners in the gulley when the winch is started without the prestart function for these scenarios. The *WaitGulleyClearTime* is thus flagged as an important input parameter, not obvious from logical reasoning, but being visible from using simulations.

It is also noted from the results that the PHEF actually increases when a low risk level miner is crossing the gulley, compared to a high risk level miner crossing the gulley (given the same risk level of winch driver used). This trend was further investigated. The behaviour of the low risk level miner crossing, is to trip (or signal to trip) the winch before crossing and the miner will rarely enter the gulley in the unsafe state. This means that more trips will be initiated from low risk level miner types before crossing, the winch will be stopped and they will enter the gulley, after which the winch driver will start the winch again (if a miner did not wait long enough) and in turn add to this prestart risk-related factor value as the winch will be started with a miner still in the gulley. As the risk level of the miner crossing increases, the miner will be less likely to trip the system (or signal to trip) and will use the gulley in the unsafe state, therefore not directly adding to the PHEF. This risk is represented in the HEF of the system.

A summary of the impact for the prestart activity is shown in Table 21 on the next page. Note that all three risk-related factors are shown for this activity, where the prestart risk-related factor (PHEF) is shown to have a significant impact on this activity.

Table 21: Activity 4 deviation analysis summary

Activity 4	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	AWS PHEF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)	ESS PHEF Impact (Change)
Experiment 8	Minimizing Activity Time (No Prestart)	AWS: No ESS: Yes	0	-0.1	1.9	0	-0.3	2.1

Observations:

- The prestart risk-related factor, PHEF, is much higher for the AWS system than for the ESS system, underlining the criticality of the prestart transitional activity. Although the impact changes of PHEF are similar for the AWS and the ESS (1.9 vs 2.1 as shown above), the absolute value of PHEF for the AWS is much larger than for the ESS (from Figure 54). Since the PHEF is significantly higher for the AWS than the ESS (in absolute terms), the mine must control this activity by using safety technology (i.e. the ESS);
- The PHEF is affected by the *WaitGulleyClear* process. This will be further investigated when Activity 12 is analysed.

6.5.8.5 Activity 5 - Trip prestart from master

Activity description:

This activity is performed by the winch driver when a *request to trip* signal has been received from the gulley during the prestart routine. In this activity, the winch driver should react to this signal and stop the prestart routine to allow a miner to cross the gulley.

Primary resources:

The primary resources involved in this activity are the miner crossing the gulley, the signalling system (AWS and ESS) and the winch driver.

For the AWS, the prestart is indicated by the driver swinging the scraper winch cables along the gulley. When a request to trip signal is received, the winch driver should stop the prestart routine and wait for the miner to cross the gulley.

In the ESS implementation, the prestart routine is performed by the system itself, and can be tripped by the winch driver when holding the “Signal” button for longer than 2 seconds. The system will go to the safe state and will not allow power to the winch.

Activity deviation experiment:

This activity is performed by the winch driver reacting to the trip signal received. The reaction time of the winch driver will not have a significant impact on the system in terms of hazardous exposure and production loss, as these times are minimal compared to the operational time. For the scenario where the reaction time (or time to stop the prestart) would take longer than the prestart duration, this will result in a critical failure as the system will then be in the unsafe state - this will then be equivalent to a failure of this activity.

Activity failure

A failure would occur when the winch driver does not stop the prestart when it has been requested from the gulley. It should be noted that this activity failure was introduced in the simulation model when using different risk level winch drivers, but the probability of failure is introduced for alternative activities, therefore a new experiment should be defined (Experiment 9) where the direct impact of this specific activity failure can be determined. In Experiment 9, for all winch driver risk types, this function always fails while the remaining resource characteristics remain unchanged.

The input parameters for this experiment can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*). Simulations were run 200 times and average results were obtained from the model response. It is noted from this experiment that the impacts on both the PLF and HEF are minimal (less than 0.1 risk-related factor change). At first this risk-related factor change seems to be less realistic and a more significant impact would have been expected, especially for the AWS. The reason for the limited impact for this activity failure was further investigated by running the simulation model real-time animation mode.

Further investigation shows the reason for the low impact is the presence of Activity 6 (Trip winch from master), where the winch is stopped by the winch driver when requested in the unsafe state. In experiment 9, the winch driver will only fail to stop the prestart when requested but the system will still be tripped / stopped when requested from the gulley in the unsafe state. Thus, the time the miner spends in the gulley in the unsafe state will show minimal change from the original experiment (experiment 1) as the system changes from the unsafe to safe state shortly after the prestart has been completed.

This shows a strong interdependency between Activity 5 and Activity 6. Thus, if a failure occurs in Activity 5, the same failure would occur for Activity 6 as both

activities use the same resources and interfaces. This could typically be for either (i) a signalling system fault or (ii) for a winch driver failure. If the signalling system should fail, the signal will not be received by the winch driver for both activities. Alternatively, if the winch driver should fail (and ignore the signal) for activity 5, he will most likely fail for activity 6. The impact of this failure will be further investigated when failures are introduced in activity 6 in the following section.

Table 22: Activity 5 deviation analysis summary

Activity 5 (Stop Prestart from master)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Experiment	Minimizing Activity Time	Yes	0	0	0	0
No experiment	Maximizing Activity Time (Relates to activity failure)	Yes	0	0	0	0
Experiment 9	WDRL 1 (Activity5 Failure)	Yes	<0.1	<0.1	<0.1	<0.1
	WDRL 2 (Activity5 Failure)	Yes	<0.1	<0.1	<0.1	<0.1
	WDRL 3 (Activity5 Failure)	Yes	<0.1	<0.1	<0.1	<0.1
	WDRL 4 (Activity5 Failure)	Yes	<0.1	<0.1	<0.1	<0.1
	WDRL 5 (Activity5 Failure)	Yes	<0.1	<0.1	<0.1	<0.1

Observations for this activity are shown below:

- This activity should be investigated together with Activity 6. Activity 6 uses the same resources and interfaces and shows a more significant impact;
- If a time deviation introduced for activity 5, it would be a maximum, this will relate to an activity failure, as simulated in experiment 9.

6.5.8.6 Activity 6 - Stop winch from master

Activity description:

This activity is performed by the winch driver when a request to trip signal has been received from the gulley when the system is in the unsafe state. In this activity, the winch driver should react to this signal and stop the winch to allow a miner to cross the gulley.

Primary resources:

The primary resources involved in this activity are the miner crossing the gulley, the signalling system (AWS and ESS) and the winch driver.

For both signalling systems, a signal will be received from the gulley to stop the winch to allow the environment to change from the unsafe to safe state. For the AWS, the winch driver should stop the winch and switch it off, while for the ESS, the winch driver can trip the system (press signal button longer than 2 seconds) which will remove power from the winch and the new system state (safe) will be indicated with green LED bezels along the gulley.

Activity deviation experiment:

This activity will also be performed when the winch driver reacts to the received signal. The reaction time of the winch driver will not have a significant impact on the system in terms of production loss, as this time is minimal compared to the duration of a shift. The miner crossing will be outside the gulley when he signals to stop the winch, thus he will not add to the HEF as this value indicates the unsafe time of miners inside the gulley. For the scenario where a miner is already in the gulley and the reaction time for the winch driver is longer, this will be considered a failure of the winch driver and a new experiment will be set up to simulate this activity failure (experiment 10).

As the probability of failure for this activity was defined in the risk type of the winch driver, experiment 10 will be set up with the failure of activity 6 to be in full, while the remaining resource activity failures are left unchanged with respect to normal operating conditions (experiment 1).

The input parameters for this experiment can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*) together with the response of 200 simulation runs. The risk-related factors for this activity as determined from experiment 10 are shown in Figure 55 on the next page.

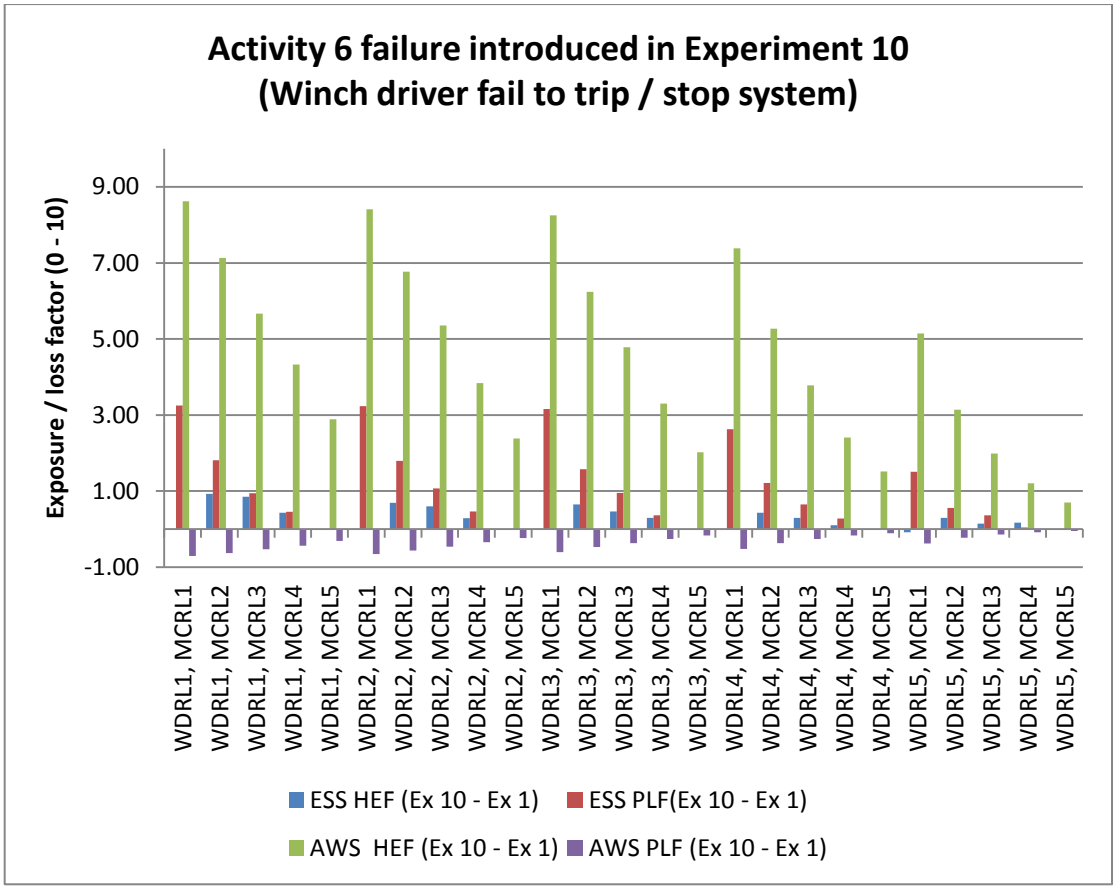


Figure 55: Activity 6 failure introduced during Experiment 10

The impact when a failure is introduced in activity 6 is shown in Figure 55. This figure indicates the difference in risk-related factors when compared to experiment 1 (normal operations).

For the ESS, this activity failure shows a slight increase in PLF (average 1.1) with a limited increase in HEF (average 0.3). When this activity fails for the ESS, the miner crossing will trip the system from the gulley when the winch driver has failed. When the system is tripped from the gulley, the winch driver should investigate the trip along the gulley – a process that can be time-consuming and adding to an increase in production loss.

The activity failure for the AWS shows a high increase in the HEF (average 4.5) while a slight decrease is shown for the PLF (average -0.36). The HEF for these scenarios where activity 6 fails, increases to 9.6 – close to the maximum. This risk change shows that if the winch is not tripped, there would be a complete system failure as there is no alternative method of stopping the winch if the requested signal from the gulley has not been acted upon or has not been communicated to the winch driver successfully. One would actually expect the HEF to increase to a maximum value of 10 when this activity fails – further investigation showed that because of the time

allocated to the *InspectSystem* process, some miners can safely cross the gulley during this time as the system is in the safe state during an inspection. This reduces the hazardous exposure slightly.

The slight decrease in production loss for this activity failure, compared to the "normal operations" experiment is due to additional time allocated to production as the winch is not stopped when requested from the gulley.

Table 23: Activity 6 deviation analysis summary

Activity 6 (Stop winch from master)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Specific Experiment	Minimizing Activity Time	Yes	0	0	0	0
Experiment 10	Maximizing Activity Time (Relates to activity 6 failure)	Yes	4.5	-0.36	0.26	1.05

Observations from this activity are listed below:

- This activity is a critical failure for the AWS (maximum hazardous exposure);
- Limited effect is seen on safety and production for the ESS.

6.5.8.7 Activity 7 - Trip prestart from gulley

Activity description:

This activity is only applicable to the ESS system as the AWS system does not provide the functionality to trip the system.

In this activity, the miner who intends to cross the gulley can trip the system when it is in the prestart state by pulling the signal cable for longer than 2 seconds. This will trip the system to the safe state allowing the miner to cross the gulley.

Primary resources:

The primary resources involved in this activity are the miner crossing the gulley and the signalling system for the ESS system (not applicable to AWS system).

As this is an automated function provided by the ESS system, there is no specific interaction required from the winch operator to perform this activity, although indication to the winch driver of the status of the system and location of the trip in the gulley will still be provided.

Activity deviation experiment:

A delayed action by the miner crossing could occur, thus introducing a delay before tripping the prestart. When this delay is less than the remaining prestart time, there will be no impact as the prestart will be tripped. If this delay is longer that the remaining prestart time, this will equate to an activity failure. Alternatively, the equipment could also fail that would result in the prestart not being tripped. This impact will also be analysed by introducing an activity failure.

The impact of an activity failure for the prestart routine would be limited, similar to the results observed from Experiment 9 where Activity 5 (Trip prestart from master) indicated that this activity has a strong dependency on Activity 6 (Trip winch from master). Thus, for the model as implemented, an activity failure for Activity 7 will have limited impact as the system will be tripped in activity 8 (Trip winch from gulley) if activity 7 (Trip prestart from gulley) would fail. The impact for activity 8 will be discussed in the following section where it will be visualised.

Table 24: Activity 7 deviation analysis summary

Activity 7 (Trip Prestart from gulley)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Experiment	Minimizing Activity Time	Yes	0	0	0	0
No experiment	Maximizing Activity Time (Relates to activity failure)	Yes	N/A	N/A	N/A	N/A

6.5.8.8 Activity 8 - Trip winch from gulley

Activity description:

Similar to activity 7, this activity is only applicable to the ESS system as the AWS system does not provide the functionality to trip the system from the gulley.

In this activity, the miner who intends to cross the gulley can trip the system when it is in the unsafe state by pulling the signal cable for longer than 2 seconds. This will trip the system to the safe state to allow the miner to cross the gulley.

Primary resources:

The primary resources involved in this activity are the miner crossing the gulley and the signalling system for the ESS system (not applicable to AWS system).

As the trip function is an automated function provided by the ESS system, there is no specific interaction required from the winch operator to perform this activity, although indication of the status of the system and gulley location of the trip will still be provided to the winch driver.

Activity deviation experiment:

If the miner crossing fails to trip the system when required, it equates to an activity failure. Similarly, if the ESS equipment is not operational and this function cannot be performed, it would be an activity failure.

This activity failure was introduced when risk levels were introduced for the miner crossing the gulley. For these resource risk levels, probabilities were defined for a failure to trip the ESS (see Section 6.5.3). Experiment 11 is defined where the probability of a miner tripping the system is set to 0% - i.e. an activity failure. Thus, the only functional routes that can be followed when the miner approaches the gulley in the unsafe state will be the “Miner fail to trip” and the miner will thus enter the unsafe gulley, or the “Miner signal to trip”, where the winch will be tripped by the winch operator.

Experiment 11 is set up as described above and, after 200 simulation runs, the average response shown in Figure 56 is obtained:

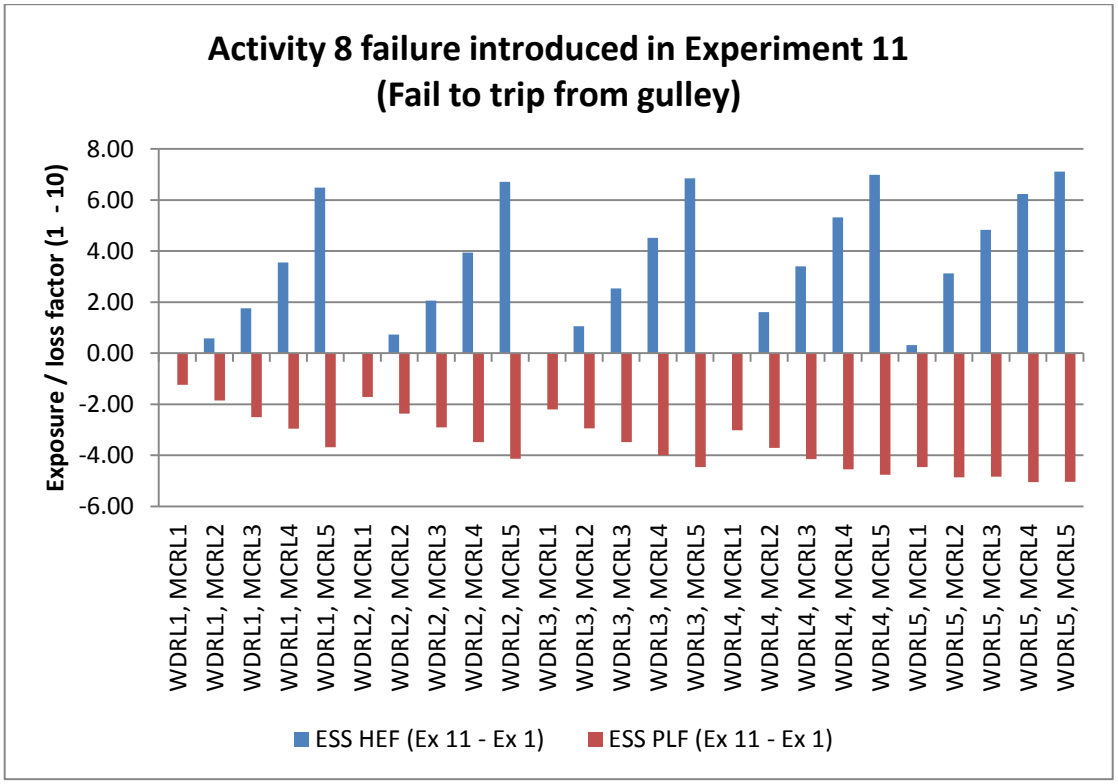


Figure 56: Activity 8 failure introduced in experiment 11

The results from Figure 56 show the risk-related factors when the *trip from gulley function* (Activity 8) fails. These results show the PLF and HEF for the ESS when compared to experiment 1 ("Normal operations").

The HEF increases significantly for this experiment (average 3.19) while the PLF decreases (average -3.54). The reason for the increase in hazardous exposure is due to the miner not being able to trip the ESS to the safe state, and the gulley will be used more frequently in an unsafe state. The decrease in production loss is due to the *InvestigateTrip* process (that may not be followed as this process is time consuming and is a major contributor to production loss).

These results show significant changes in risk-related factors for this activity and shows that this activity contributes significantly to a reduction in hazardous exposure (compared with the AWS and ESS in experiment 1). The impact for this activity is summarised in the table below.

Table 25: Activity 8 deviation analysis summary

Activity 8 (Trip winch from gulley)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Experiment	Minimizing Activity Time	Yes	NA	NA	0	0
Experiment 11	Maximizing Activity Time (Relates to activity failure)	Yes	NA	NA	3.19	-3.54

Observations from this analysis are listed below:

- This activity is not present in the AWS;
- This activity increases the hazardous exposure significantly for the ESS;
- The increase in production loss is due to the *InvestigateTrip* process, to be analysed in Activity 14.

6.5.8.9 Activity 9 - Start the winch

Activity description:

In this activity, the winch driver will start the winch to proceed with scraping. This activity is performed in exactly the same way for both the AWS and ESS and is an activity performed within the *DoProductionProcess*. The ESS controls power to the winch with power only present when the ESS is in the unsafe state. This has no direct impact on this specific activity, or in the way this activity is performed.

Primary Resources:

The primary resources in this activity are the winch driver and the scraper winch itself. The signalling system is not a primary resource for this activity.

Activity deviations:

As the signalling system is not a primary resource for this activity, this activity is performed in the same way for both systems. Therefore this activity will not be analysed with a specific experiment.

If this activity should fail completely, production will not be possible. For this same failure, the hazardous exposure will decrease to a minimum as the environment will not be in the unsafe state.

A deviation in time (delay) to perform this activity will have no material impact on the comparison between systems. If a delay were introduced, less time will be allowed for production (increase in production loss) while the environment will be safe for the same amount of time longer due to a decrease in hazardous exposure.

Table 26: Activity 9 deviation summary

Activity 9 (Start the winch)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No Experiment	Minimizing Activity Time	No	0	0	0	0
No Experiment	Delayed Activity Time	No	Proportional to delay	Proportional to delay	Proportional to delay	Proportional to delay
No experiment	Maximizing Activity Time (Relates to activity failure)	No	Maximum	Maximum	Maximum	Maximum

The observation for this activity is as follows:

- The signalling system is not a primary resource for this activity, therefore the impact for any deviation introduced will be similar for both systems.

6.5.8.10 Activity 10 - Scrape ore

Activity description:

In this activity the winch driver should operate the winch to scrape ore along the centre gulley. Similar to activity 9, this activity is performed in exactly the same way for both the AWS and ESS as implemented in the *DoProductionProcess*.

Primary Resources:

The primary resources in this activity are the winch driver, the scraper winch and the environment. Note that the signalling system is not a primary resource for this activity. The interfaces for the winch operator to the controls of the winch will also remain the same.

Activity deviations:

As the signalling system is not a primary resource for this activity, this activity is performed in the same way for both systems. Therefore, this activity will not be analysed for a specific model.

If this activity should fail completely, production will not be possible, leading to a maximum increase in PLF. For this same failure, the HEF will decrease to a minimum as the environment will not be in the unsafe state.

A deviation in time (delay) to perform this activity will have no differential impact. The impact for both systems will be proportional to the length of delay introduced.

Table 27: Activity 10 deviation analysis summary

Activity 10 (Scrape ore)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Risk Change)	AWS PLF Impact (Risk change)	ESS HEF Impact (Risk Change)	ESS PLF Impact (Risk Change)
No Experiment	Minimizing Activity Time	No	0	0	0	0
No Experiment	Delayed Activity Time	No	Proportional to delay	Proportional to delay	Proportional to delay	Proportional to delay
No experiment	Maximizing Activity Time (Relates to activity failure)	No	Maximum	Maximum	Maximum	Maximum

An observation for this activity is given below:

- The signalling system is not a primary resource for this activity, therefore the impact for any deviation introduced will be similar for both systems.

6.5.8.11 Activity 11 - Signal gulley crossed

Activity description:

Activity 11 requires the miner crossing the gulley to signal to the winch operator that the gulley has been crossed and that production can proceed. This activity is performed for both signalling systems.

Primary Resources:

The primary resources in this activity are the miner crossing, the winch driver and the signalling system.

When the ESS is used, the miner crossing will signal to the winch driver using audio-visual signalling. The location of the signal will be visible on the status display of the ESS control unit. With the AWS, a strain wire is used to signal. Only audible indication will be used for signalling to the winch operator.

Activity deviations:

A deviation for this activity was introduced in the human resource risk levels defined for the miners crossing the gulley (see Table 14). As the resource risk level for the miner crossing the gulley increases the likelihood increases that the miner will not signal to the winch operator that the gulley has been crossed. This means that the time the winch operator waits for the gulley to clear will eventually time out – this is discussed in the following section in the analysis of activity 12 (as performed in experiment 12).

Typically, this activity will not be delayed in normal operations as the miner who crossed the gulley will proceed to his destination. In experiment 12, the probability of failure for this activity is set to 100% for all resource types representing the miner crossing the gulley. The remaining resource characteristics stay as defined in Table 14.

Experiment 12 used 200 runs for all resource type combinations and both signalling systems. The results from this experiment were compared with the results of experiment 1 (normal operation) to determine the impact of this activity. The results showed a minimal impact change on both production and hazardous exposure, which appeared to be similar for both systems. The detailed results for this experiment can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*).

There is a slight increase in production loss for both systems, as expected. This is because the production process is delayed when miners crossing do not signal to the winch driver to resume scraping operations. This delayed production is shown in the increase in PLF, but the change value is less than 0.2 as this delayed time is a small fraction of the total production time set for the simulation run (8 hours). The impact for this activity is summarised in Table 28 on the next page.

Table 28: Activity 11 deviation analysis summary

Activity 11 (Signal gulley crossed)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
Experiment 12	Activity failure	Yes	<0.1	<0.2	<0.1	<0.2

Observations for this activity are as follows:

- The impact of this activity is minimal and similar for both systems;
- A slight increase in production loss is evident with the failure of this activity.

6.5.8.12 Activity 12 - Wait for gulley to clear

Activity description:

This activity is present for both the ESS and AWS. In this activity, the winch operator waits for the miner to cross the gulley before the winch driver continues with operations.

Primary Resources:

The primary resources involved in this activity are the winch driver, the signalling system, and the miner crossing. When the winch is stopped by the winch driver upon request from the gulley, the winch driver should wait for a signal from the miner crossing to indicate when the gulley has been crossed to allow scraping. This activity is implemented in the same way for both signalling systems.

Activity deviations:

Deviations for this activity were introduced as the winch driver risk level. The average time for this activity is set to 60 seconds with deviation (in both directions) depending on the resource risk level. This deviation is defined in Table 13, and increases as the risk level of the winch driver increases.

The impact is determined by disabling this activity in experiment 13. This is achieved by setting the *WaitGulleyClearTime* to 0 in the *WaitGulleyClear* process. The input parameters and results for experiment 13 can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*). This experiment was run for 200 replications and the results, when compared to experiment 1, are shown in Figure 57 on the next page.

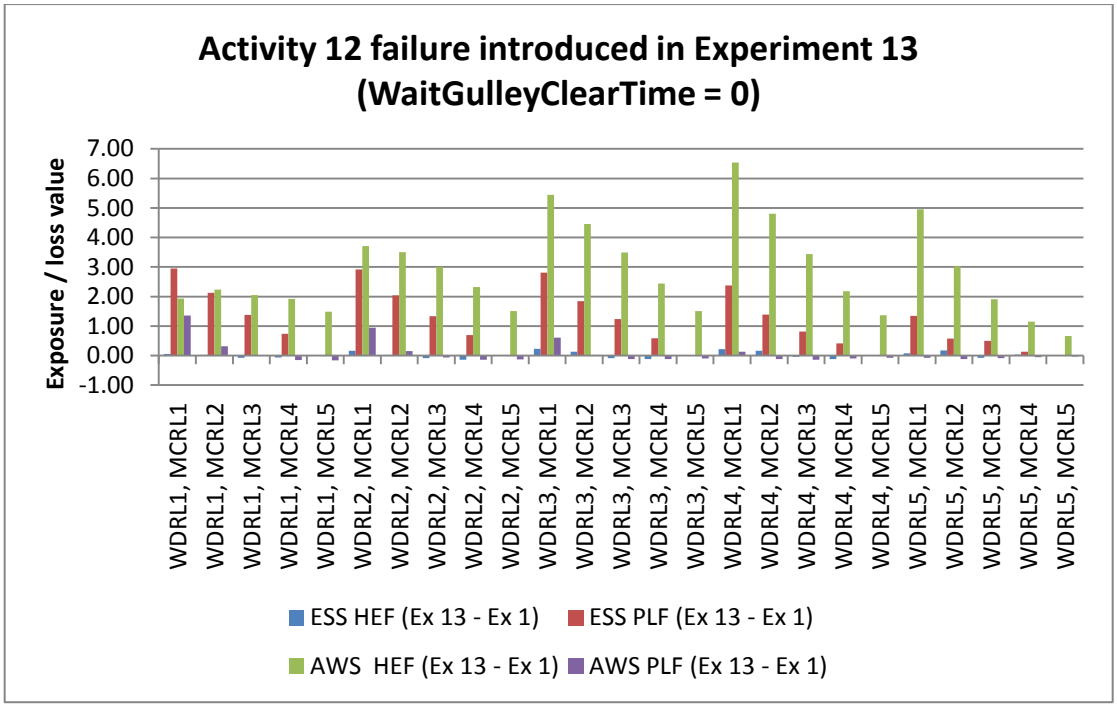


Figure 57: Activity 12 failure introduced in experiment 13

The results from Figure 57 show a significant impact on the risk-related factors. For the AWS, a large increase in HEF is seen (average 2.8) while the change in PLF for the AWS is minimal (average 0.07). In the ESS, this activity contributes to the PLF (average 1.1) while the HEF impact is minimal (average 0.02).

The increase in hazardous exposure for the AWS is due to the winch being started shortly after the miner enters the gulley as there is no hold-off period and no fixed prestart routine for the AWS. In the ESS, the prestart routine is fixed and allows for the miner to trip the system to a safe state from the gulley, if necessary. This, in turn, is the reason for the increase in production loss for the ESS, as more system trips will be initiated from the gulley with this activity disabled. Increased trips result in increased trip investigations (Activity 13) which this is a time consuming activity and loss in production. The sensitivity for activity 13 is analysed in the following section.

Both the HEF and PLF increases shown in Figure 57 show a maximum when the miner crossing is of risk level 1 with a reduced increase when the miner's risk level increases for a fixed risk level winch driver. This is due to higher risk-related factors for high risk level resources in experiment 1 against which the comparison is made – a higher risk increase is thus evident for the lower risk level resources.

In Section 6.5.8.4, in the analysis of activity 4 (Do Prestart), it was found that a deviation in the PHEF is quite sensitive to the different resource risk type parameters introduced for activity 12, the *WaitGulleyClearTime* parameter. To determine this impact, the PHEF for experiment 1 and Experiment 13 are compared in Figure 58 on the next page.

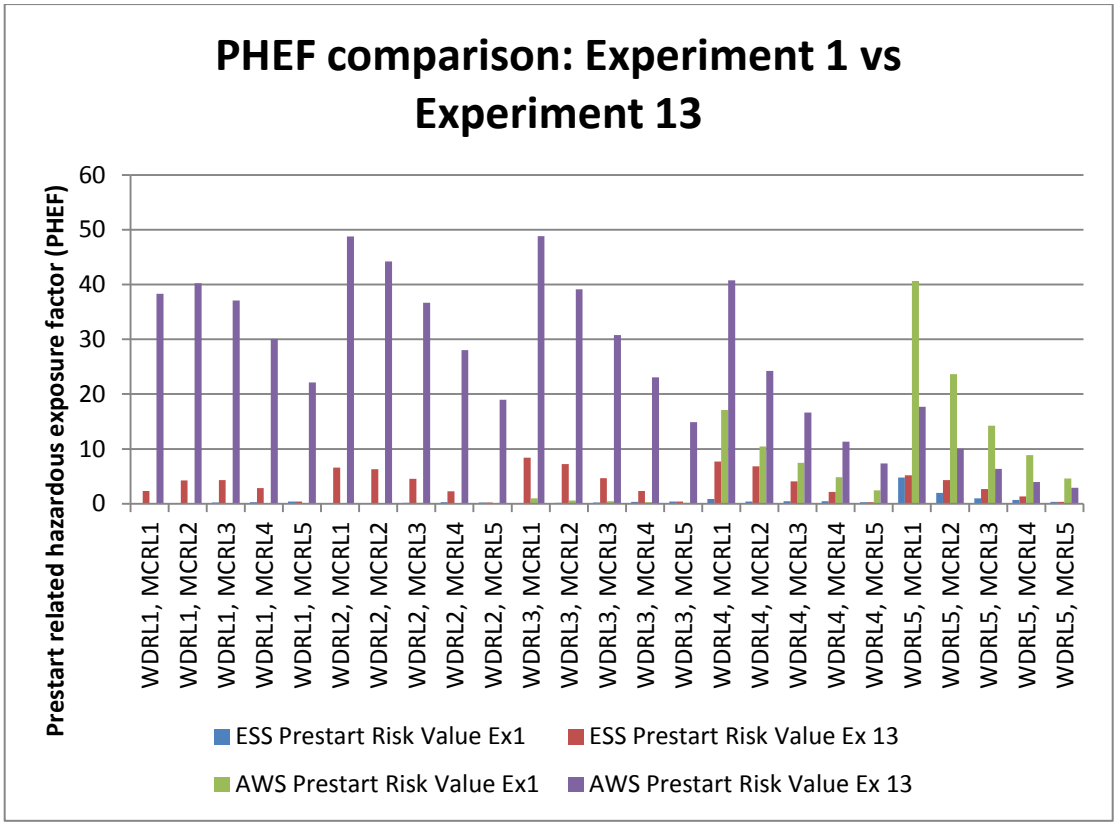


Figure 58: PHEF comparison: Experiment 1 vs Experiment 13

The significant impact of activity 12 on the PHEF is confirmed from the results of experiment 13 as shown in Figure 58. The PHEF for the AWS increases from an average of 5.5 (Exp1) to an average of 25.7 (Exp 13) while the PHEF for the ESS increases from an average of 0.6 (Exp1) to an average of 3.7 (Exp 13). Note that this value represents the number of occurrences out of a 100 miners crossing when the system was started with a miner inside the gulley. Thus, for the AWS with a failure of activity 12, 25% of miners crossing the gulley will be inside the gulley when the winch is started.

The results determined in this section mean that a failure of this activity has a significant impact on the system safety and prestart related hazardous exposure. These are summarized in the table below:

Table 29: Activity 12 deviation analysis summary

Activity 12 (Wait for gulley to clear)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	AWS Prestart Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)	ESS PHEF Impact (Change)
Experiment 13	Minimizing Activity Time (WaitGulley ClearTime = 0)	Yes	2.84	0.07	20.19	0.02	1.13	3.11

Observations for activity 12 are as follows:

- Additional hazardous exposure is introduced in the AWS for this activity;
- Additional production loss is introduced for the ESS;
- This activity shows a high sensitivity with respect to the prestart risk-related factor, particularly for the AWS.

6.5.8.13 Activity 13 - Investigate trip

Activity description:

This activity is only applicable to the ESS. In this activity, the environment must be investigated whenever the system has been tripped from the gulley.

Primary Resources:

The primary resources involved in this activity are the winch driver and the signalling system. The winch driver must determine the location of the tripped slave unit along the gulley. This is indicated by means of an LED display on the ESS control unit. Once the location has been determined, the winch operator must walk / crawl up the gulley to investigate the event. With all in order, the system must be reset at the involved slave unit, after which the winch operator must walk / crawl back to the scraper winch. If the system has not been reset at the tripped slave unit, the system will prevent the winch operator from scraping.

Activity deviations:

Time deviations were introduced for this activity in the risk levels for the winch operator. These deviations are set using a random triangular function for the *InvestigateTripTime* of the *InvestigateTrip* process. The minimum time for this activity is allocated to the winch driver risk level 1 (*Random.Triangular(2,8,20)*) where an average of 8 minutes are allowed. The maximum time for this activity is allocated to the risk level 5 winch driver (*Random.Triangular(2,12,40)*) where an average of 12 minutes are allowed (this is, of course, for a high risk winch driver). The complete definition of the winch driver risk types is given in Table 13.

Although time deviations were introduced in experiment 1 (the normal conditions experiment), a new experiment will be defined (experiment 15) where the time for this activity is set to 30 minutes (with no randomness) for all resource risk types. The remaining characteristics of the resource risk types remain as for experiment 1.

Experiment 15 was simulated using 200 runs with input parameters as defined above. The complete set of input parameters with the responses can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*). The results in terms of impact for this experiment are shown in Figure 59 on the next page.

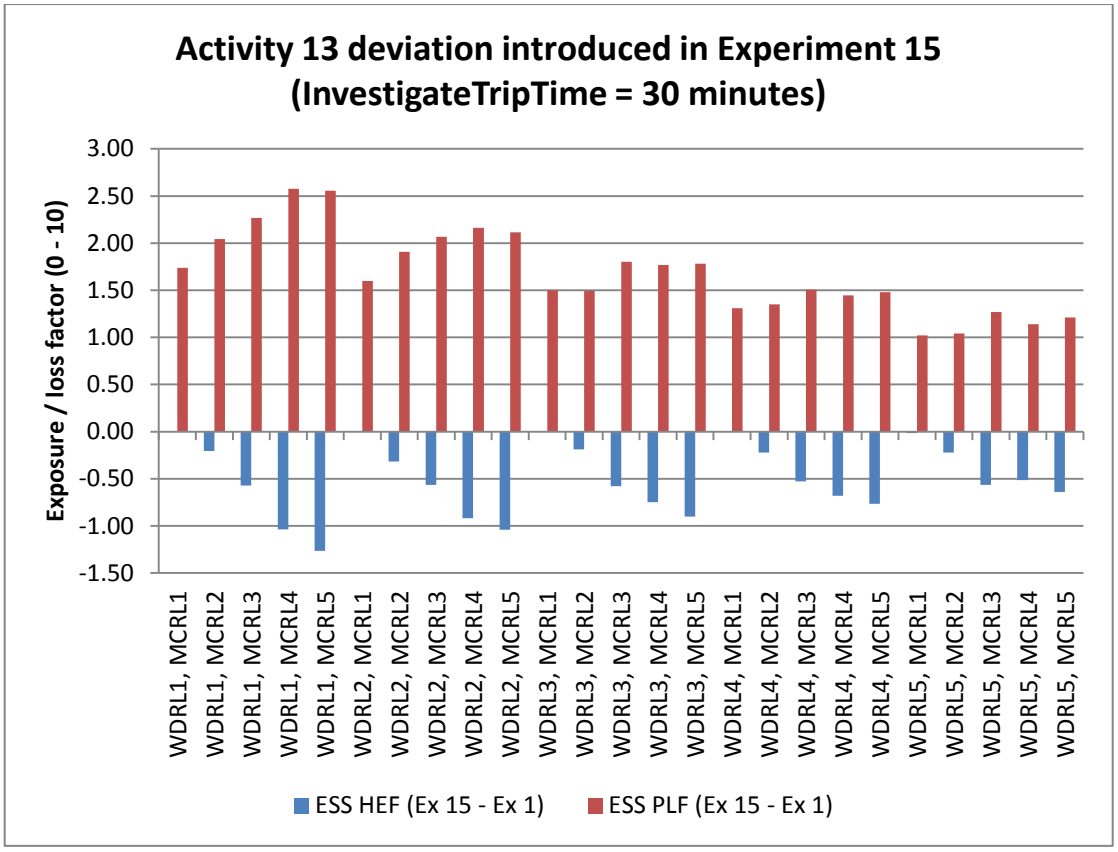


Figure 59: Activity 13 deviation introduced in experiment 15

Figure 59 shows the impact for this activity deviation when compared to experiment 1 (the normal conditions activity). It is clear that this deviation causes a significant increase in PLF (avg 1.7). This is because no production can be performed when this activity is being executed. There is also a decrease in the HEF for this activity (average 0.5), this is due to the gulley being in a safe state during this activity. During investigation, any miner crossing the gulley will be in the safe state, hence the decrease in hazardous exposure.

This activity is quite sensitive with respect to production loss. To determine this sensitivity, it is necessary to investigate the impact if this activity were not performed, i.e. removing this activity from the workflow (with this activity removed, the ESS will be equivalent to the AWS). This activity is effectively removed in experiment 16, where the *InvestigateTripTime* for this activity is set to 0. Experiment 16 uses 200 simulation runs. The risk-related factors for this experiment re compared with the factors of experiment 1, with differences shown in Figure 60.

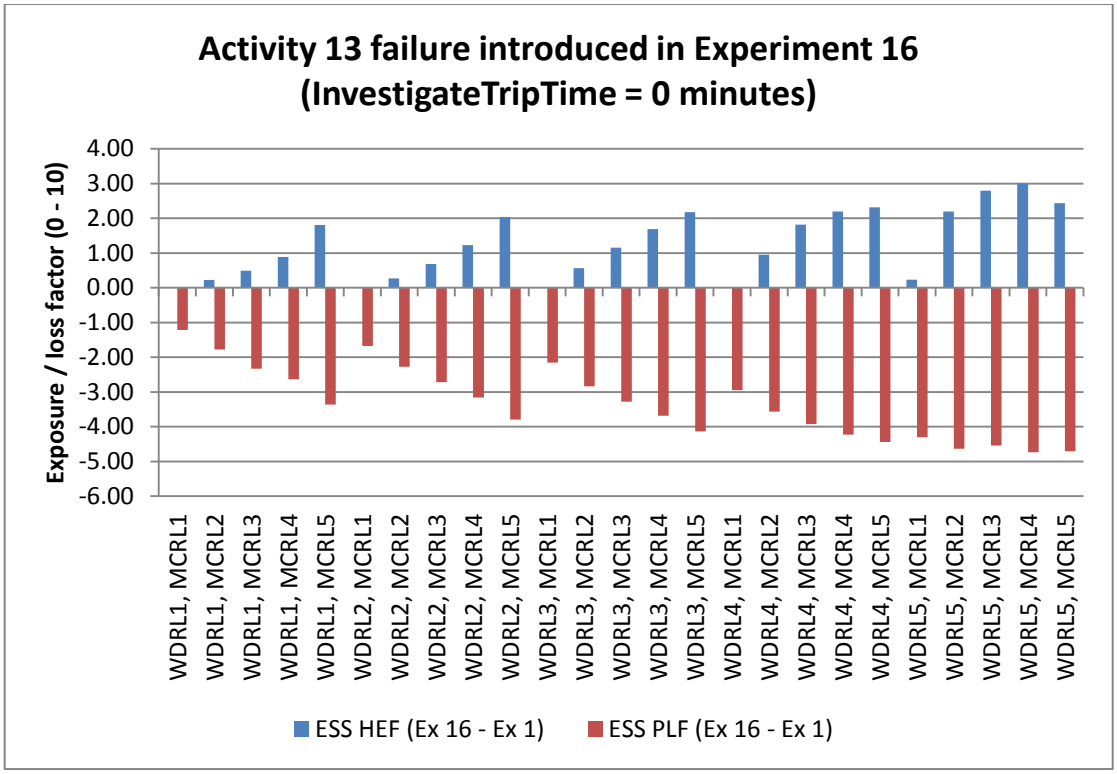


Figure 60: Activity 13 failure introduced in experiment 16

Figure 60 shows significant impact on the risk-related factors when this activity has failed. A decrease in PLF is notable (average 3.3) while there is a relatively small increase in HEF (average 1.2). The decrease in production is due to the long inspection time during which production is suspended. The increase in hazardous exposure is due to the increased number of miners crossing the gulley while the system is in production, as opposed to crossing the gulley during the *InvestigateTrip* process. The increase in hazardous exposure correlates with higher risk level miners.

This experiment shows that higher production losses for the ESS system, compared to the AWS in experiment 1, are mainly due to the winch driver investigating trip conditions.

A third deviation can be introduced for this activity in terms of an activity failure. If the winch driver fails to investigate a tripped condition, the system cannot enter the prestart routine until the tripped condition has been reset on the slave unit at the tripped location along the gulley. This means that no further production can be performed while the system (environment) is in the safe state. For this activity failure, the system will fail to a safe state. The hazardous exposure impact for this activity failure will therefore be minimum while the production loss impact will be maximum.

The deviations introduced in this analysis shows that the PLF for the ESS is sensitive with respect to this activity failure. The summary from this analysis can be found in Table 30.

Table 30: Activity 13 deviation analysis summary

Activity 13 (Investigate Trip)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
Experiment 16	Minimizing Activity Time (Activity disabled)	Yes	NA	NA	1.2	-3.3
Experiment 15	Delayed Activity Time (30 minutes)	Yes	NA	NA	-0.5	1.7
No experiment	Activity failure	Yes	NA	NA	Minimum	Maximum

Observations from this analysis are listed below:

- The production loss factor (PLF) is sensitive with respect to failure of this activity failure;
- Winch operator risk types have significant effect on the production loss of this activity.

6.5.8.14 Activity 14 - Reset system

Activity description:

This activity is only available for the ESS. This activity is performed as part of activity 13 where a system trip from the gulley should be investigated. This activity represents the resetting of the system along the gulley at the location of the trip.

Primary Resources:

The primary resources involved in this activity are the winch driver and the signalling system.

Activity deviations:

Time deviations for this activity were introduced as part of the resource risk type for the winch operator. These time deviations are set in the *InvestigateTripTime* process as discussed in the previous section in the analysis of activity 13.

A failure of this activity implies the system cannot enter the prestart state before scraping as the system fails in a safe state which, in turn, will have maximum impact on production with minimum impact on hazardous exposure. No specific experiment will be run to show this impact as this effect was shown in the first experiments. The summary for the impact for this activity is shown in Table 31 on the next page.

Table 31: Activity 14 deviation analysis summary

Activity 14 (Reset system)	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Impact (Change)	AWS PLF Impact (Change)	ESS HEF Impact (Change)	ESS PLF Impact (Change)
No experiment	Activity failure	Yes	NA	NA	Minimum	Maximum

An observation from this analysis is shown below:

- The system will fail to safe when this activity fails, resulting in a production loss.

6.5.8.15 Activity-based risk summary (ABR Step 9)

Results from the activity-based risk analysis are summarized in Table 32 on the next page. This table shows the impact for all activities assessed using ABR and simulations. This impact is shown in terms of production loss (PLF) and hazardous exposure (HEF), with prestart-related hazardous exposure (PHEF) shown where applicable.

Production loss and hazardous exposure are loss ratios measured on a normalized scale of 0 – 10 while prestart-related exposure is measured as the number of instances where a miner had been in a gulley during prestart over 100 simulation runs.

The exposure / loss factors shown in the table are the differences between a specific activity's loss factors and the loss factors of experiment 1, which represents normal operational performance.

Table 32: Activity-based risk summary for AWS and ESS

	Experiment	Experiment Description (Deviation)	Signalling System Prim Resource?	AWS HEF Change	AWS PLF Change	AWS Prestart Change	ESS HEF Change	ESS PLF Change	ESS Prestart Impact
Activity 1 (Do Pre-shift Inspection)	Exp 2	Minimizing Activity Time	**Yes**	<0.2	<0.2	NA	<0.2	<0.2	NA
	Exp 3	Maximizing Activity Time	**Yes**	<0.2	<0.2	NA	<0.2	<0.2	NA
	Exp 4	Activity failure (operations proceed while system faulty)	**Yes**	**4.6**	0.5	NA	-1.5	**5.8**	NA
Activity 2 (Identify whether ore should be scraped)	Exp 5	Minimizing Activity Time	No	<0.2	<0.2	NA	<0.2	<0.2	NA
	Exp 6	Maximizing Activity Time	No	<0.2	<0.2	NA	<0.2	<0.2	NA
	No Exp	Activity failure 1: (operations proceed while no ore is present)	No	Fair	None	NA	Limited	None	NA
		Activity failure 2: (operations do not proceed while ore is present)	No	None	Fair	NA	None	Fair	NA
Activity 3 (Determine environment state)	No Exp	Minimizing Activity Time	**Yes**	0	0	NA	0	0	NA
	No exp	Maximizing Activity Time	**Yes**	0	0	NA	0	0	NA
	Exp 7	MCRL 1	**Yes**	NA	NA	NA	NA	NA	NA
		MCRL 2	**Yes**	**1.4**	-0.1	NA	0.9	0.5	NA
		MCRL 3	**Yes**	**2.9**	-0.3	NA	**1.7**	0.9	NA
		MCRL 4	**Yes**	**4.3**	-0.5	NA	**2.5**	**1.3**	NA
		MCRL 5	**Yes**	**5.8**	-0.6	NA	**3**	**1.7**	NA
Activity 4 (Do Prestart)	Exp 8	Minimizing Activity Time (No Prestart)	AWS: No **ESS: Yes**	0	-0.1	1.9	0	-0.3	2.1
Activity 5 (Stop prestart from master)	No Exp	Minimizing Activity Time	**Yes**	0	0	NA	0	0	NA
	No exp	Maximizing Activity Time (Activity failure)	**Yes**	0	0	NA	0	0	NA
	Exp 9	WDRL 1 - 5 (Activity Failure)	**Yes**	<0.1	<0.1	NA	<0.1	<0.1	NA

Activity 6 (Stop winch from master)	No Exp	Minimizing Activity Time	**Yes**	0	0	NA	0	0	NA
	Exp 10	Maximizing Activity Time (Activity failure)	**Yes**	**4.5**	-0.36	NA	0.26	**1.05**	NA
Activity 7 Trip prestart from gulley	No Exp	Minimizing Activity Time	**Yes**	0	0	NA	0	0	NA
	No exp	Maximizing Activity Time (Activity failure)	**Yes**	N/A	N/A	NA	N/A	N/A	NA
Activity 8 Trip winch from gulley	No Exp	Minimizing Activity Time	**Yes**	NA	NA	NA	0	0	NA
	Exp 11	Maximizing Activity Time (Relates to activity failure)	**Yes**	NA	NA	NA	**3.19**	**-3.54**	NA
Activity 9 (Start the winch)	No Exp	Minimizing Activity Time	No	0	0	NA	0	0	NA
	No Exp	Delayed Activity Time	No	$\propto$ delay	$\propto$ delay	NA	$\propto$ delay	$\propto$ delay	NA
	No exp	Maximizing Activity Time (Activity failure)	No	Max	Max	NA	Max	Max	NA
Activity 10 (Scrape ore)	No Exp	Minimizing Activity Time	No	0	0	NA	0	0	NA
	No Exp	Delayed Activity Time	No	$\propto$ delay	$\propto$ delay	NA	$\propto$ delay	$\propto$ delay	NA
	No exp	Maximizing Activity Time (Activity failure)	No	Max	Max	NA	Max	Max	NA
Activity 11 (Signal Gulley crossed)	Exp 12	Activity failure	**Yes**	<0.1	<0.2	NA	<0.1	<0.2	NA
Activity 12 (Wait for gulley to clear)	Exp 13	Minimizing Activity Time (WaitGulleyClearTime = 0)	**Yes**	**2.84**	0.07	**20.19**	0.02	**1.13**	**3.11**
Activity 13 (Investigate trip)	Exp 16	Minimizing Activity Time (Activity disabled)	**Yes**	NA	NA	NA	1.2	-3.3	NA
	Exp 15	Delayed Activity Time (30 minutes)	**Yes**	NA	NA	NA	-0.5	1.7	NA
	No exp	Activity failure	**Yes**	NA	NA	NA	Min	Max	NA
Activity 14 (Reset system)	No exp	Activity failure	**Yes**	NA	NA	NA	Min	Max	NA

It is clear from this activity-based risk summary that HEF and PLF measures are more sensitive to failures and deviations in specific activities. It was also observed that combinations of activities may have higher impact when compared to individual activities. The activities more sensitive to deviations and failures are highlighted in Table 32. Where HEF and PLF increased significantly, cells in the table are highlighted red while scenarios where HEF and PLF decreased, cells are highlighted green. Where a signalling system is not the primary resource, cells are not highlighted because deviations and failures in these activities will have similar impact on both systems. Activities that showed high HEF, PLF, and PHEF sensitivity with respect to deviations or failures are discussed in the following paragraphs.

- Activity 1 (Do pre-shift inspection): If the signalling system should fail and operations proceed - the AWS would fail to an unsafe state while the ESS system would fail to safe. The AWS system will add significant hazardous exposure while production loss is introduced in the ESS, as the ESS does not allow production when the system fails.
- Activity 3 (Determine environment state): This activity showed an HEF that is more sensitive for the AWS than for the ESS. This is due to the clear indication of the environment state given by the ESS while the AWS shows no indication of the environment state (safe, unsafe, or prestart).
- Activity 4 (Do prestart): A failure of this activity resulted in limited impact on HEF and PLF. However, as this is a transitional state, a prestart-related exposure factor was defined as an additional hazardous exposure had been identified, namely the presence of a miner in an unsafe gulley during prestart. There is similar increase in the PHEF for both systems when the prestart is disabled in the model. This is therefore an important activity required for the signalling system. The impact of this activity becomes more evident when this activity is disabled in a combination with activity 12.
- Activity 6 (Stop winch from master): A failure of this activity shows a high HEF change / impact with an increase of 4.5 for the AWS. The ESS shows an HEF impact of 1.1. This is due to the ESS allowing for the system to be tripped directly from the gulley, giving the miner control over safety. This activity is the only way to stop a winch when the AWS is in use as no trip functionality is provided from the gulley.
- Activity 8 (Trip winch from gulley): This activity is not present in the AWS system. In the analysis of this activity, it became evident that this activity contributes significantly to safety of the ESS but also affects production. This

trip function provides a secondary safety control and allows a miner crossing to trip the winch directly, thus decreasing hazardous exposure. When the system is tripped from the gulley during this activity, the trip must be investigated by the winch operator. This investigation is a time-consuming process adding significantly to production loss.

- Activity 12 (Wait for gulley to clear): This activity analysis shows significant sensitivity of the HEF and PHEF with respect to failure for the AWS. This is mainly due to the AWS that has no fixed prestart routine. For the ESS, a limited production loss and PHEF is introduced, while the increase in production loss is due to more trips initiated from the gulley (investigated by the winch driver in Activity 13) when this activity fails.
- Activity 13 (Investigate trip): This activity turned out to be the main contributor to production losses – PLF – of the ESS. When this activity is disabled, the simulation results showed that an additional 33% of a total shift can be spent on the *DoProduction* process. Due to a significant increase in production time (unsafe operations) hazardous exposure increases slightly.
- Activity 14 (Reset system): If this activity fails, the ESS system fails to a safe state and no production would be possible. Therefore production losses are at maximum while hazardous exposure will be at minimum. This is because no unsafe operations are allowed by the ESS.

6.5.9 System trade-off analysis (ABR Step 10)

As shown from the results from experiment 1, the AWS has high hazardous exposure while production loss is limited when compared to the ESS where production loss is higher and hazardous exposure less.

High risk activities were identified in the previous step where system analysis was carried out in terms of activity-based risk. When focusing on high risk activities, one can perform a trade-off by addressing these activities specifically in terms of the loss factors defined in the previous section, or use a combination of low risk activities from both systems. Thus, information from studying embedded risk for each activity is an invaluable contribution to the signalling system trade-off.

Two steps will be taken for the trade-off analysis. In the first step, risk reduction will be done on high risk activities to find a system with the lowest risk. This system will be defined as the electronic signalling system 2 (ESS2). In the second step, cost reduction will be done on high cost activities to result in the system with the lowest

cost. Thus, the risk-reduced system (ESS2) will be cost-reduced to result in an alternative system, the electronic signalling system 3 (ESS3).

In reducing cost, the risk factors (HEF and PLF) would typically increase, but the trade-off is done to determine a point where an acceptable balance between hazardous exposure and cost has been found.

6.5.9.1 Electronic signalling system 2 definition (ESS2)

It is clear from the results, when the AWS and ESS were compared, that the ESS proved to be a significantly safer system, but production was compromised quite significantly. The focus on the trade-off that follows is to use functions / activities from the first electronic signalling system (ESS) as a framework for the ESS2, and to address activities that contribute to the production loss in the process. Once this new system configuration has been defined (ESS2), the new system configuration can be simulated in the updated simulation model to determine the impact of the new system.

In the ESS2, high risk activities of the ESS are addressed as follows:

- The Investigate trip activity (Activity 13) resulted in significant production loss with the ESS. This activity is not present in the AWS (as the system cannot be tripped) and production loss of the AWS is thus significantly lower. This activity will be removed for the ESS2 (together with the system reset function – Activity 14), and will thus allow a winch operator to proceed with operations after a trip without investigating the area;
- It was seen from the risk analysis of Activity 12, that the Wait for gulley to clear activity has a safety impact in terms of the PHEF if the activity time is at minimum. This results in a winch driver not waiting for the miner to cross the gulley and proceeding with a prestart. In the ESS2, this activity will be set to 30 seconds and controlled by the signalling system itself. This means that the signalling system will ignore a prestart from the winch operator when it is done within 30 seconds of the last system tripped event. This delay gives the miner in the gulley sufficient time to complete a crossing.

When using the generic signalling system model, as shown in Figure 40 and Figure 41, the process representing activity 12, where the gulley is allowed to be cleared, is only implemented when the winch has been stopped by the master. When activity 13 (Investigate trip) is removed from the system, activity 12 should also be present when the system is tripped from the gulley to allow the miner to cross the gulley before the

system is started again. Thus, for ESS2 the *InvestigateTrip* process is replaced with another *WaitGulleyClear* process, which is set to 30 seconds.

The system architecture, layout and interfaces remain unchanged for the ESS2, as was presented in Figure 32, Figure 33 and Figure 34. The only physical change to the system is the reset function on the slave / signalling units along the gulley as activity 13 has been removed.

6.5.9.2 ESS2 simulation results

Experiment 17 is set up to represent the system configuration for the ESS2. The complete set of input and response parameters can be found on the accompanying compact disc (*Winch Signalling System Case Study Experiments Information.pdf*). The following figures show the direct comparison for all three systems in terms of the hazardous exposure factor (HEF) and production loss factor (PLF).

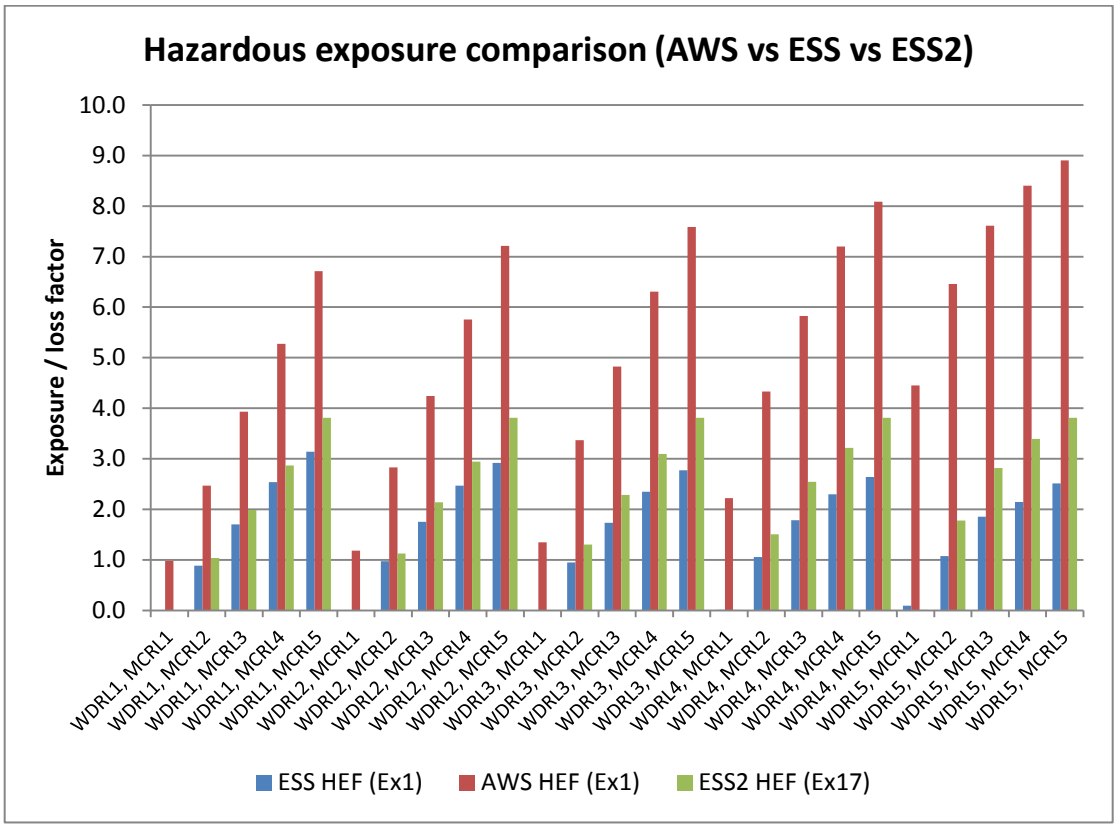


Figure 61: HEF comparison for ESS2

The hazardous exposure factor (HEF) for three system configurations are shown in Figure 61. The HEF for ESS2 (average 2.1) is still significantly lower than for the AWS (average 5.1). It is noted that the HEF for ESS2 has increased slightly as compared to the ESS (average 1.6) even though the HEF activities are similar for both these systems. This increase in HEF is due to the investigate trip activity

(Activity 13) being removed. With this activity not present, more production is performed resulting that the system is longer in the unsafe state. When this activity was present in the ESS, the system had been in a safe state during the time a system trip had been investigated, meaning that miners could cross the gulley in a safe state while an investigation was being performed.

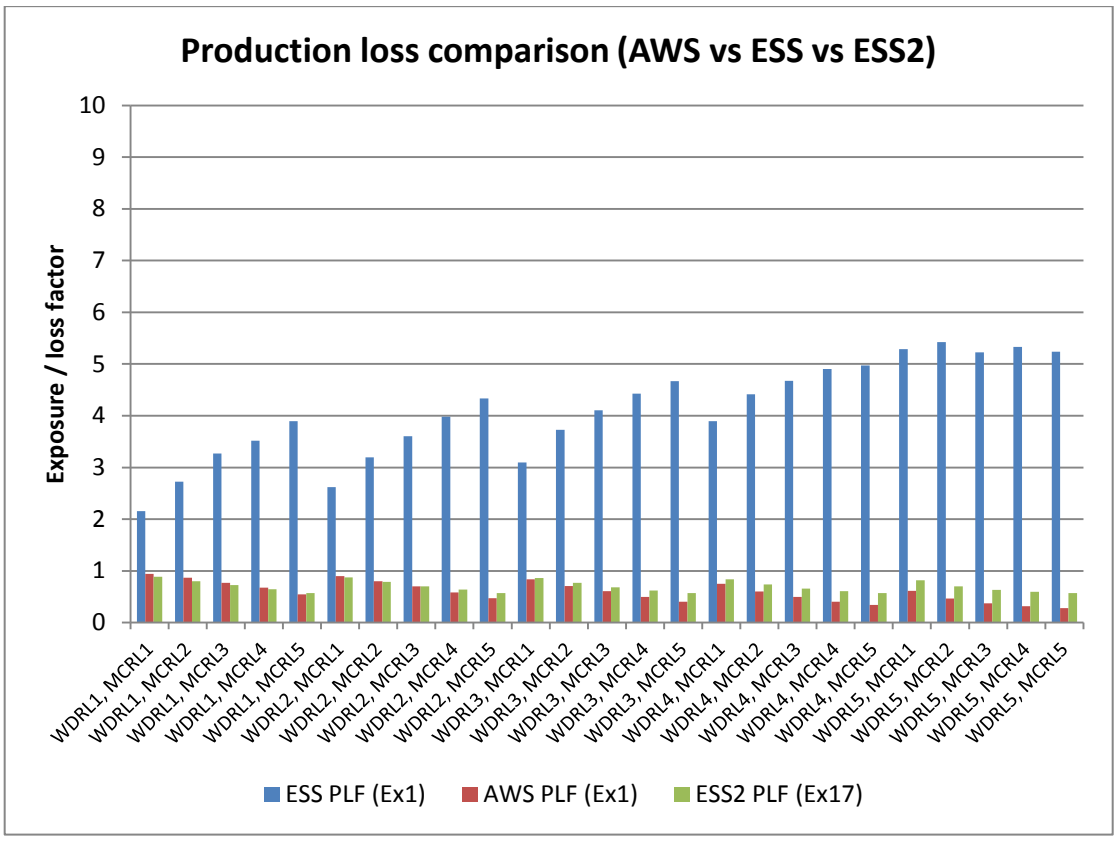


Figure 62: PLF comparison for ESS2

The production loss comparison for the three system options are shown in Figure 62. The ESS2 (average 0.7) shows a significant decrease in PLF when compared to the initial ESS (average 4.1). This PLF for the ESS2 is similar to the low PLF determined for the AWS (0.6).

In the detailed analyses where activity-based risk was analysed, the prestart-related hazardous exposure factor (PHEF) was introduced to determine the number of miners that were in a gulley when the system changed from safe to unsafe states. It is important to also determine the PHEF for the ESS2. The PHEF (for ESS2) is given in Figure 63 on the next page.

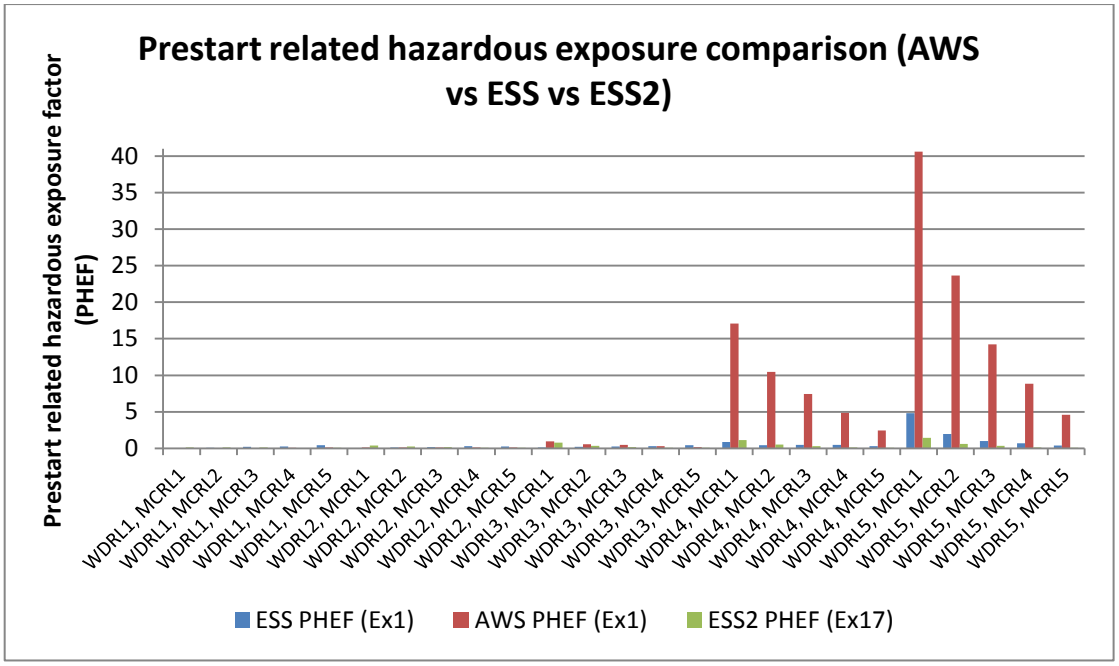


Figure 63: PHEF comparison for ESS2

It is clear from Figure 63 that the PHEF present in the ESS has been reduced significantly in this risk reduced configuration process. The ESS2 systems shows almost no PHEF, due to the adaptation of activity 12 (Wait gulley clear) which now employs a 30s fixed delay, controlled by the signalling system and not the winch driver.

6.5.9.3 ESS2 trade-off summary and findings

The simulation results for the risk reduced system (ESS2) are discussed in the previous section. From these results the following conclusions can be drawn:

- The hazardous exposure of the ESS2 is slightly elevated when compared to the ESS, but is significantly lower when compared to the AWS. This slight increase is due to increase in production time (unsafe time) of the system because activity 13 had been removed;
- The production loss is significantly lower in the ESS2 when compared to the ESS, but is similar to the low PLF for the AWS;
- The prestart related hazardous exposure has been significantly reduced with the introduction of a fixed delay for activity 12, controlled by the signalling system and not the winch operator.

Given these findings, it is clear that the high production loss and hazardous exposure activities from the ESS system have been addressed by modelling a risk-reduced system (as defined for ESS2) through the activity-based risk process.

An alternative system (ESS3) is introduced in the following section. For this system, the impact of removing / altering costly activities is investigated.

6.5.9.4 Electronic signalling system 3 definition (ESS3)

The previous section presented a risk-reduced solution (ESS2) and was evaluated in terms of the hazardous exposure factor (HEF), production loss factor (PLF), and prestart-related hazardous exposure factor (PHEF). In this section, the risk-reduced ESS2 system is cost-reduced.

The AWS is a simplistic system in terms of equipment when compared to the ESS. This means that one of the main cost drivers of the ESS (and ESS2) system is the use of multiple slave units for signalling and status indication along the gulley. The approach to reduce the cost of the system is to reduce the number of components in the system, that is, to reduce equipment features. This can be done by reducing the number of signalling units along the gulley and to only use a master unit at the location of the winch, with a single slave unit on the opposite side to provide signalling and trip functionality from both sides of the gulley. This system solution will be analysed as the electronic signalling system 3 (ESS3).

The new system layout and system architecture are presented in on the next two pages.

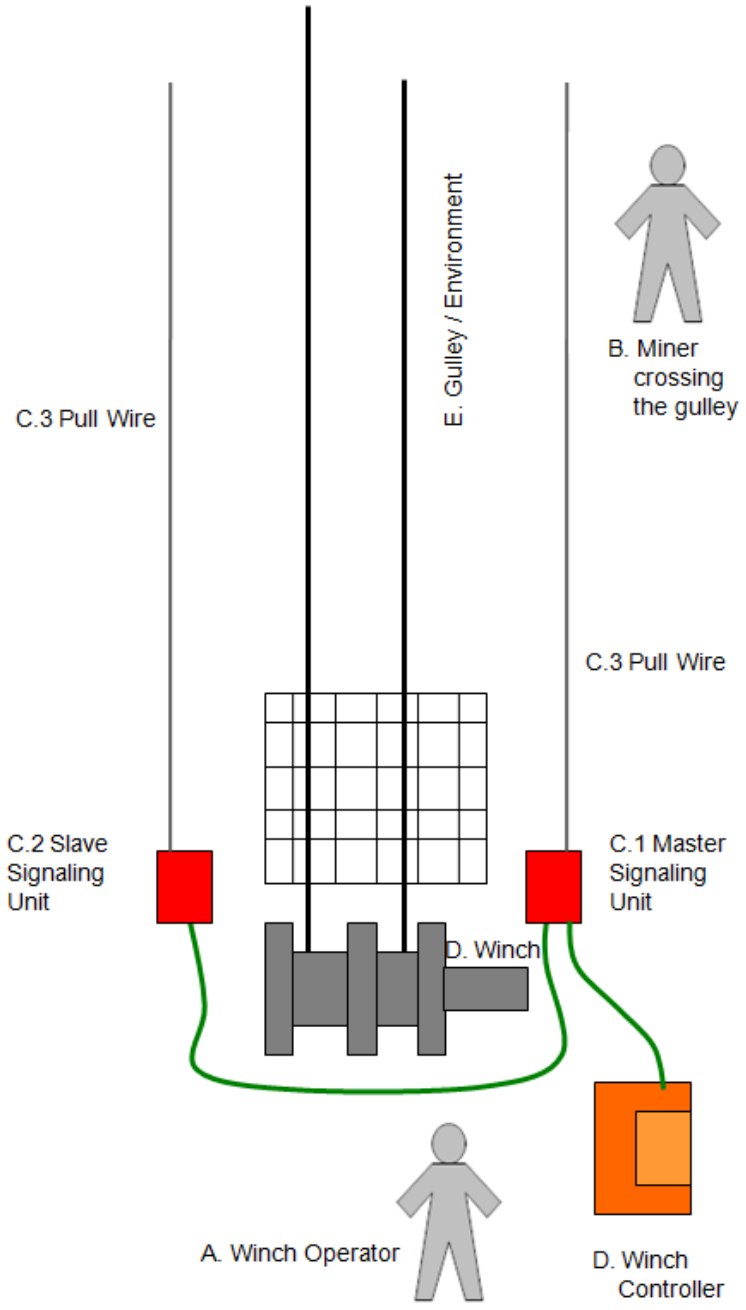


Figure 64: Electronic signalling system 3 architecture

The system architecture of the ESS3 is shown in Figure 64. The resource configuration (apart from the absence of more slave units) and functions remain as defined in the functional analysis above.

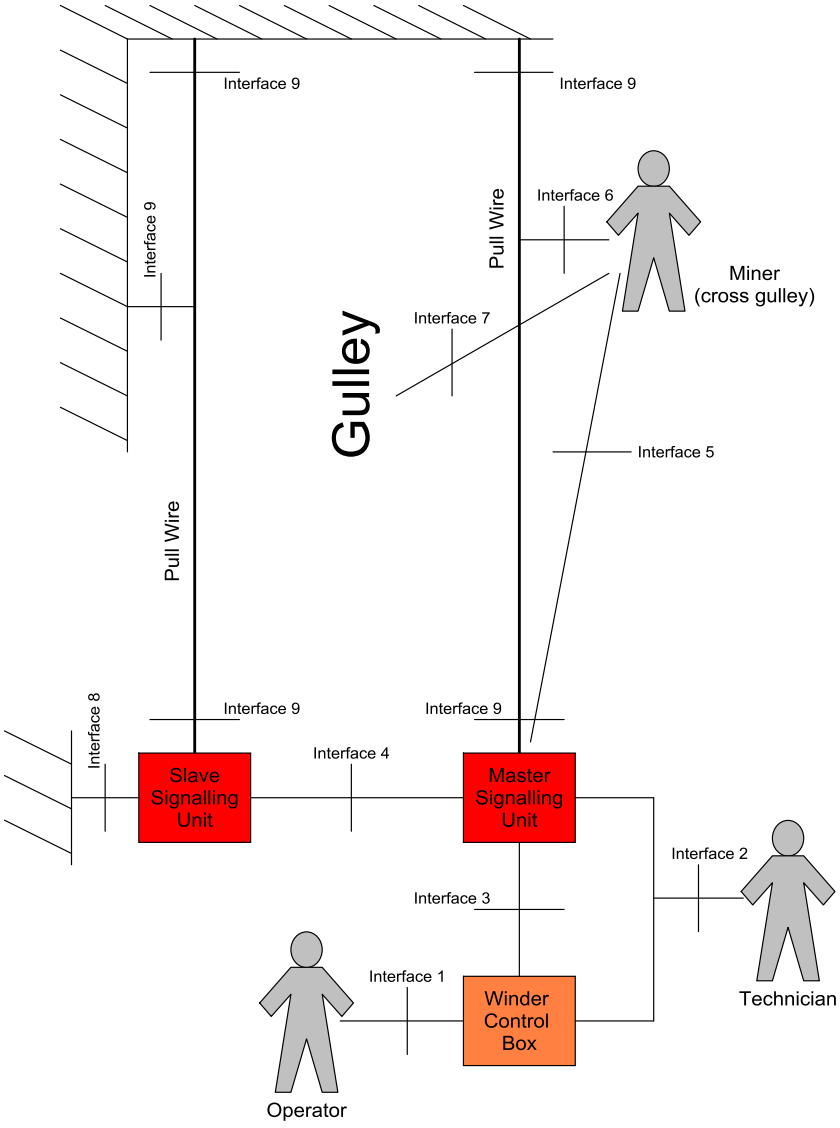


Figure 65: Electronic signalling system 3 interfaces

The interfaces of the new system (ESS3) are shown in Figure 65. These interfaces are numbered in the same order as the interfaces in Section 6.4.2.2 with differences between interfaces indicated below:

Interface 1 – Winch Operator to Winch Control Box interface

This interface is the same as for the ESS.

Interface 2 – Winch operator to master signalling unit interface

This interface is similar as for the ESS, except for the status display representing the status of the signalling units that is not available to this option (only one slave unit is used).

Interface 3 – Master signalling and winder control box interface

This interface is the same as for the ESS.

Interface 4 – Interconnection between signalling units

This cable is only used for electrical connection and does not serve as the pull cable as used in the ESS (and ESS2).

Interface 5 – Miner crossing and slave signalling unit interface

This human-machine interface is similar but is only available at the winch. The visual and audible indications are not used along the gulley.

Interface 6 – Miner crossing and pull wire interface

This interface is similar as for the ESS, but a strain wire is used in the ESS3 instead of an electrical pull cable.

Interface 7 – Miner crossing and gulley / environment interface

This interface is similar to the ESS, but no status indication is used along the gulley.

Interface 8 – Mounting of signalling units

Only one signalling unit is used with mounting similar to the ESS.

Interface 9 – Strain wire connection and support

This interface is similar as for the ESS, but a strain wire is used instead of a pull cable. The strain wire is supported along the gulley, connected to a pull switch at the one end (signalling and master unit) and terminated at the end of the centre gulley.

The activities used for the ESS3 are the same as for the ESS2, but limited indication of the system state is available along the gulley. This influences decisions made by miners crossing the gulley with added impact with respect to the ESS. This option still allows a miner to signal and trip from the gulley as a continuous signal wire will be used along the gulley (similar to the AWS).

The same simulation model used for the ESS2 will be used to determine the impact of the ESS3 as the ESS2 has been risk-reduced. As the interfaces in ESS3 differ (from Figure 65) the input parameters in terms of routes followed by human resources differ from ESS2. The volatility table for the winch driver is similar to the volatility table defined in Table 13 (for the ESS). The interface between the system and miner has changed for the ESS3 because no signalling units are present along the gulley. The volatility values for the miner crossing are defined in Table 33. Signalling to the winch driver that the gulley has been crossed (Activity 11) has not changed as this activity is not influenced by the interface difference. The probability for this specific activity remains as defined in Table 14.

Table 33: Miner type crossing the gulley volatility table (ESS3)

Resource type: Winch driver	**Activity 11: Signals to the driver to trip the system**			**Activity 7 and 8: Trips the system from the gulley**			**Activity 7 and 8 altenative action: Uses the gulley in the unsafe state**		
	AWS	ESS and ESS2	ESS3	AWS	ESS and ESS2	ESS3	AWS	ESS and ESS2	ESS3
Deviation function	Stochastic			Stochastic			Stochastic		
1 (Good miner)	90%	80%	75%	0%	20%	20%	10%	0%	5%
2 (Above average miner)	75%	60%	55%	0%	30%	30%	25%	10%	15%
3 (Average miner)	60%	40%	35%	0%	40%	35%	40%	20%	30%
4 (Below average miner)	45%	20%	20%	0%	50%	40%	55%	30%	40%
5 (Poor miner)	30%	0%	0%	0%	60%	45%	70%	40%	55%

The probability values for the deviation function from Table 33 are adjusted to account for differences in interfaces between the ESS and ESS3. The changed activities mainly relate to system status indication. The AWS system provides no system status indication, while status indication is clearly defined by the ESS and ESS2 by the master and slave units along the gulley. The status indication in the ESS3 is present, but limited as the system status is only indicated at the winch itself. This status indication consists of an LED bezel as part of the master unit. The status indication may be visible from the gulley but is not as clear as for the ESS and ESS2. Therefore, the probability values for the ESS3, defining probabilities of routes followed by the miner crossing, fall between the values for the AWS and ESS.

6.5.9.5 ESS3 simulation results

The generic simulation model is used as a basis for the ESS3 simulation. The same system functionality is used, with the difference between the ESS2 and ESS3 being the resource volatility table for the miner crossing the gulley. The resource parameters from Table 33 are used for this option.

The simulation model for the ESS3 is defined in experiment 18. This experiment uses averages over 200 iterations, with risk-related factors of the ESS3 compared to prior models (AWS, ESS and ESS2). These results are discussed in the following paragraphs.

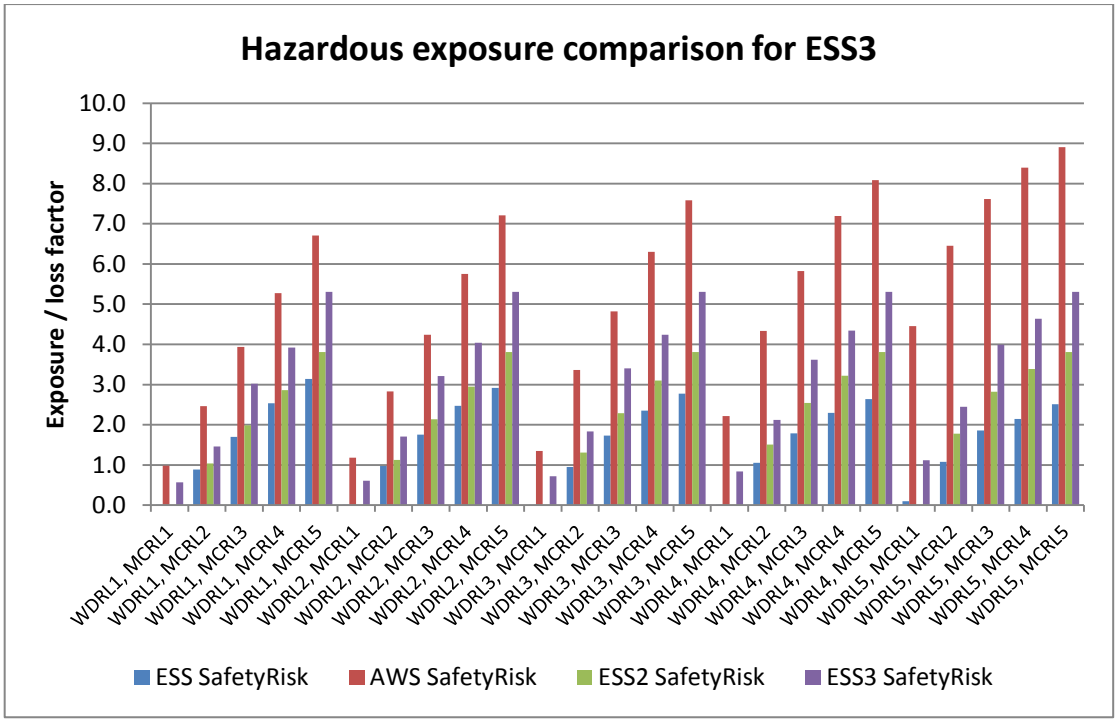


Figure 66: HEF comparison for ESS3 simulations

The HEF values for the ESS3 are illustrated in Figure 66. As expected, the HEF has increased in general when compared to the ESS2 and ESS, but is it still lower than the risk shown for the AWS system. The increase in HEF is due to the interface change in the ESS3, indicating the importance of system status indication when using a signalling system.

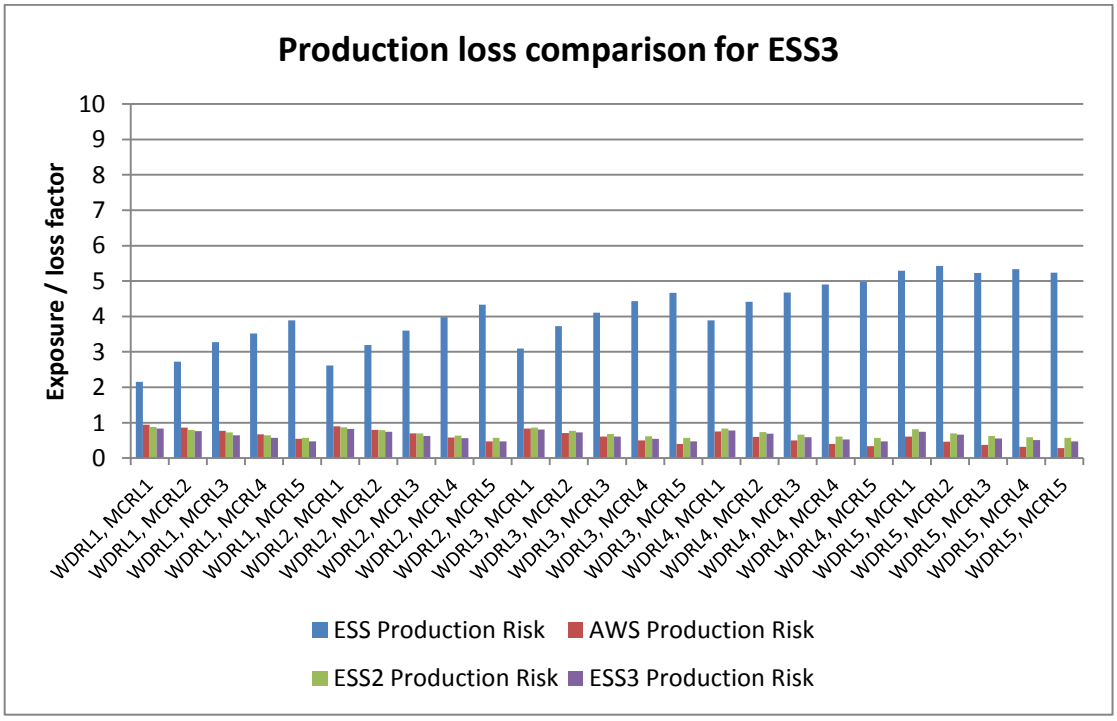


Figure 67: PLF comparison for ESS3

The PLF values for the ESS3 are presented in Figure 67 on the previous page. The PLF for the ESS3 is fairly low and similar to the PLF of the AWS and ESS2. The ESS system shows a high production loss factor, which has been addressed in the ESS2.

The prestart related hazardous exposure factors (PHEF) were also determined from simulations the ESS3. The PHEF for the ESS3 is not shown as it is the same as for the ESS2.

6.5.9.6 ESS3 trade-off summary and findings

The ESS3 is defined as an alternative system with the focus on cost reduction. The analysis of this system was discussed in the previous section. From these results the following conclusions can be made:

- The HEF of the ESS3 has increased when compared to the ESS2, but is significantly lower when compared to the AWS. This loss factor increase is due the interface of the ESS3 limiting status indication and signalling along the gulley. Thus, system status indication is present at the winch but not explicitly present along the gulley;
- The PLF is relatively low for ESS3, similar to the low PLF shown for the AWS and ESS2;
- The prestart-related hazardous exposure is still very low for the ESS3, and is similar in value to the PHEF determined for ESS2. This is due to the introduction of a fixed waiting time for activity 12 controlled by the signalling system and not the winch operator.

System analysis for the ESS3 shows the results for a low-cost electronic signalling system solution. The ESS3 system shows higher hazardous exposure when compared to the ESS2 system due to the absence of status indication along the gulley.

The system is a trade-off between risk and cost. Both the ESS2 and ESS3 meet the minimum requirements as set out by the MHS act and can be used in the mining environment, although the ESS2 will provide lower hazardous exposure.

The electronic signalling system is a risk control measure. To increase the effectiveness of this risk control, additional controls must be implemented. These controls relate mainly to organizational policy changes, leading to cultural changes in terms of safety, management processes, and procedures and discipline.

6.6 System detail design and implementation (ABR Step 11)

Detail development and implementation were done as part of this case study to verify consistency of the ABR process. From the development of equipment for the first system, parameters were observed and applied for operational modelling of the ESS – that is, the model was derived from requirements and underground observations. The ABR acquisition process was also developed in parallel with the development of the ESS, and was formalised in this part of the research.

The second and third models – the ESS2 and ESS3 models – were developed from the adjusted theoretical models as discussed above. Therefore, the ESS2 and ESS3 models verify the changes made to risk- and cost-reduce the original ESS. Since the first model parameters were obtained from actual observations, these parameters were also used when modelling the ESS2 and ESS3 systems and the resulting equipment.

Three separate electronic signalling systems were developed in this research. The first system addresses the initial requirements (ESS) as set out by the South African mine, while the second and third systems are the risk-reduced (ESS2) and cost-reduced (ESS3) solutions as determined from the ABR process. In following the ABR process, functional and physical characteristics of all the systems were determined. These characteristics were used as input to the detail design and development phase.

Detailed information on the equipment design is not presented in this document as the focus of this research is to research, design and verify an acquisition process. However, the results from the development of the ESS, ESS2 and ESS3 are presented in summary in this section as their implementation was used to verify the ABR acquisition process.

The ESS solution is the most complex system and is presented in most detail first, after which the ESS2 and ESS3 are presented as physical realisations of functional subsets of the ESS.

6.6.1 Electronic signalling system (ESS) development

The electronic signalling system presented in this section addresses the requirements of the initial specification provided by the mine to replace the air whistle system (AWS). The ESS equipment presented in this section was thus developed from the key requirements as set out in Table 10 and complies with the functional analysis performed in Section 6.4.2. This solution is regarded as the most complex solution with a comprehensive feature set as presented in the following sub sections.

6.6.1.1 System components (ESS)

The equipment consists of a control unit (C.1), signalling unit (C.2), signal cable (C.3), and access key. The layout and physical configuration are shown in Figure 32 and Figure 33. Each of these developed system components is presented and discussed in the following paragraphs.

Control Unit (C.1)

Shown below is the control unit which is located at the winch. Each of the items on the unit is described after which functional definitions of components are given.

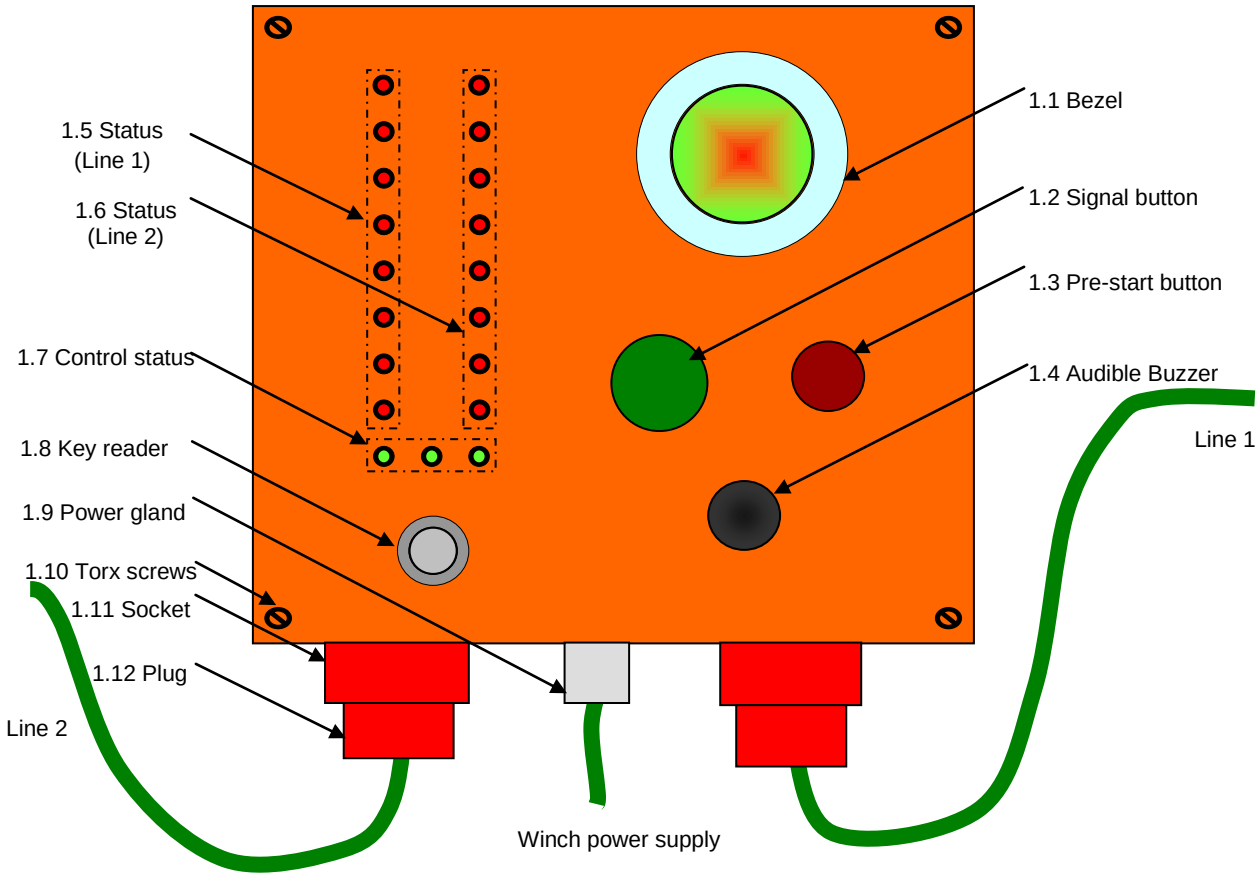


Figure 68 - ESS control unit (C.1)

1. The display bezel (1.1) is an LED display that is used to indicate safe and unsafe conditions to a winch operator. Two colours are displayed under normal operational circumstances, namely red for unsafe conditions and green for safe conditions;
2. A green signal button (1.2) is used to signal to the rest of the signalling boxes. Signalling means that buzzers will sound and LED bezels will flash accordingly;
3. The winch start button (1.3) is used to start the winch system. Pressing this button enables the winch to operate following a pre-start routine;

4. An audible buzzer (1.4) is located on the front panel and is used to sound when a cable is pulled or when the signal button (1.2) is pressed;
5. Two rows of status indicators (1.5 for line 1 and 1.6 for line 2) are used to indicate the status of the system, namely if a cable is being pulled, when a trip condition has occurred, or when a signalling unit (or units) or cable is faulty;
6. The control status indicator (1.7) is a set of 3 indicators used to indicate the status of the master unit and cables. An indicator on the left that steadily flickers indicates that the control unit is active. The remaining indicators are used to indicate faults on the cables such as over current and open cables that result in communications errors and short circuit conditions;
7. A key reader (1.8) is provided to control access to the control unit. This is done to ensure authorised use of the system and each operator must have access to his / her own key;
8. Power is fed to the control unit from the winch power supply. This cable enters the control unit through a compression gland;
9. All units are closed using Torx screws (1.10) to prevent unauthorized access to the inside of the unit. A technician will require a Torx screw driver to open the enclosure of the unit;
10. Two cable sockets (1.11) are provided for the two communications lines. Cables are connected to the control unit by inserting the cable plug (1.12) into the mating socket.

The representation of the developed solution is shown in the image below:

Figure 69: ESS control unit

The image on the left shows the front view of the control unit for the ESS. This image corresponds to the representation in Figure 68. The image on the right shows the internal view with all developed circuits integrated in the control unit enclosure.

Signalling Unit (C.2)

The signalling units are located on two communications lines (left and right) and are installed along a gulley. There can be up to eight signalling units on each of the two communications lines (1 and 2) giving a total of 16 signalling units. A representation of the signalling unit, located on a straining wire is shown in the following figure:

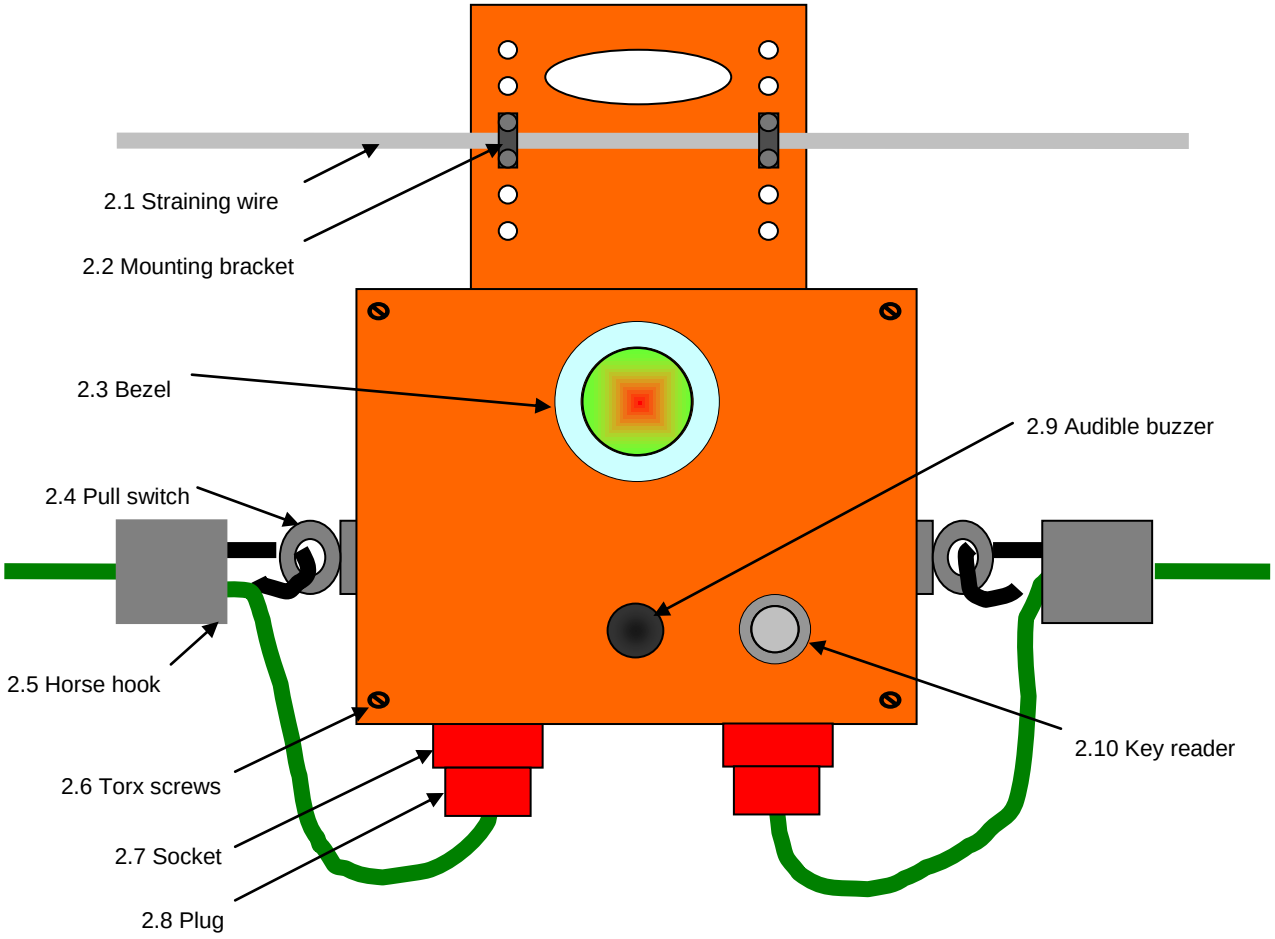


Figure 70: ESS signalling unit (C.2)

1. A signalling unit is mounted on a straining wire (2.1) along a gully. Each signalling unit is mounted to the wire by means of mounting brackets (2.2). Since signalling units will be transported by hand, a carry-handle is provided in the mounting flange at the top;
2. The display bezel (2.3) displays red for unsafe conditions (the winch is active), green for safe conditions (the winch is inactive), or both red and green if the signalling unit is faulty;
3. Pull switches (2.4) located on the right- and left-hand sides of the signalling unit are used for signalling or tripping a winch. Each pull switch is connected to a

communications cable by means of a horse-hook (2.5) that serves to relieve strain on the cable plug (2.8) and to apply strain to the pull switch instead;

4. Torx screws (2.6) are used to prevent unauthorized personnel from opening the signalling units and a Torx screw driver is required to open the enclosure;
5. A receiving socket (2.7) for the cable plug is located on the bottom panel of the signalling unit and receives a mating cable plug (2.8) for normal use;
6. There are 3 audible buzzers (2.9) on the signalling unit, with one buzzer located in front and two buzzers located on the side panels. These buzzers are aimed down the centre gully and towards a strike gully as sound is directional at this frequency (3 kHz) - this gives thorough coverage in all directions;
7. A key reader (2.10) is provided on the front panel of the signalling unit for resetting a trip condition. Only authorized keys are allowed to reset a trip condition.

The representation of the developed signalling units is presented in the following image:

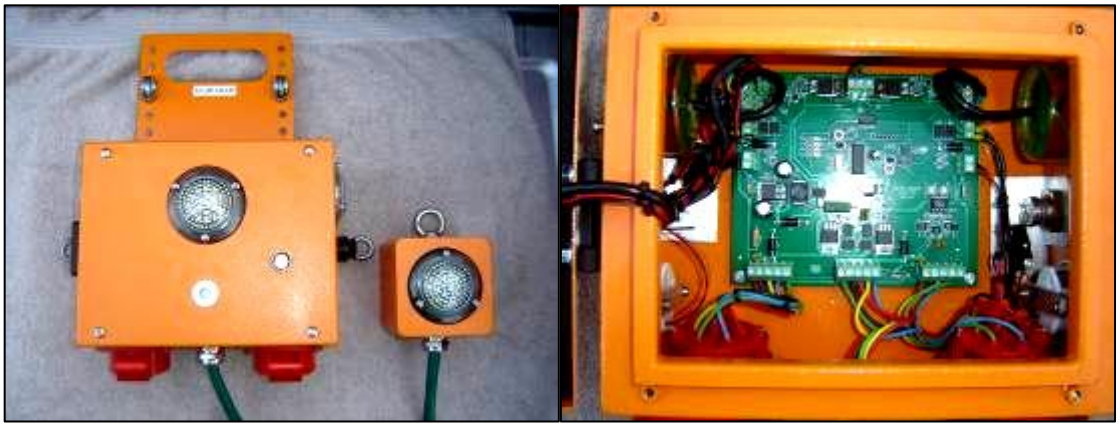


Figure 71: ESS implemented signalling unit

The image on the left shows the front view with of the signalling unit and corresponds with Figure 70. The image on the right shows the internal circuit board integrated in the signalling unit enclosure.

Signal Cable (C.3)

Reinforced cables are used to connect a master unit to signalling units. A reinforced cable as shown in Figure 72 on the next page is used, specifically designed for pull-cable applications. Pigtails support the cables to a suitable safe operating height on each side of the gulley while tail-ends allow for access to pull cable in deep gulley conditions.

Figure 72: Reinforced signal / interconnection cable

Access key

Identification buttons are used to provide access to a winch through the signalling system. The same access key needs to be used to reset a signalling unit along the gulley upon a system trip.

6.6.1.2 System interfaces (ESS)

A basic interconnection diagram (see Figure 73) below shows the interface arrangement of a master unit and a signalling unit for the ESS system.

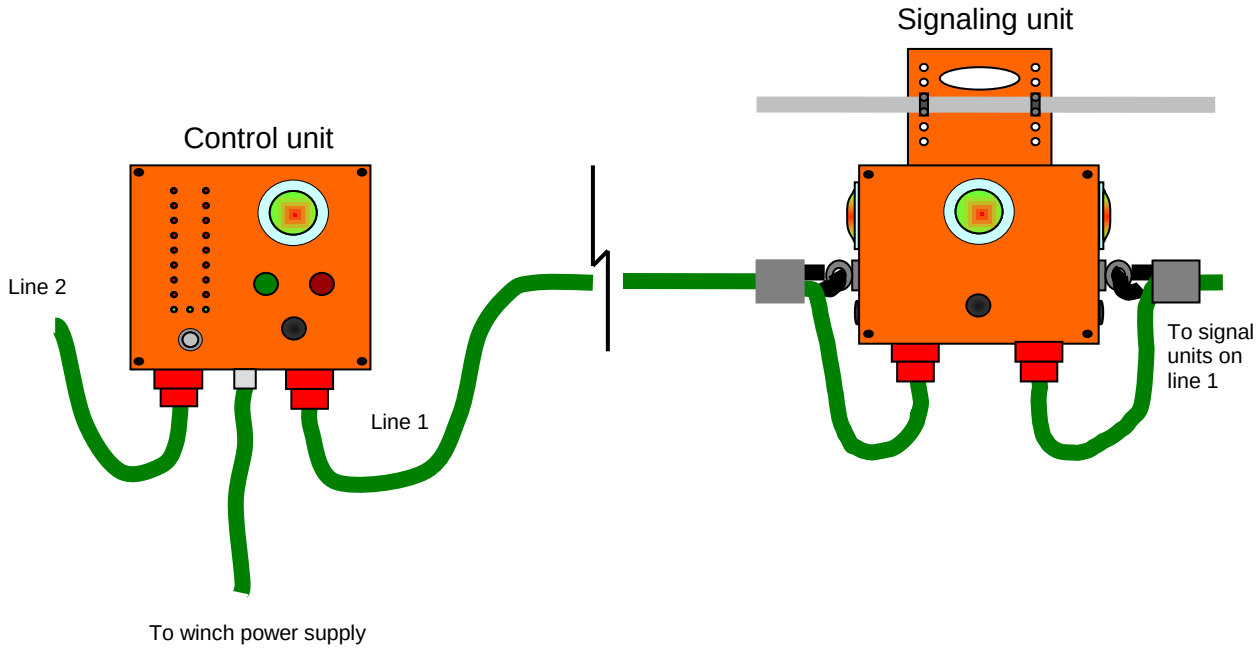


Figure 73 - Control unit and signalling unit interface diagram

The system interfaces were defined in Figure 34 of Section 6.4.2.2. The corresponding interfaces specific to the system design are discussed in this section:

Interface 2 - Human-machine interface between a winch operator and control unit;

Interface 3 - Interface between the winch power supply and the control unit;

Interface 4 - An interconnection cable between winch signalling units;

Interface 5 and 6 - Human-machine interface between signalling unit and signal cable.

Each of these interfaces shall be described in the following sections.

Interface 2 - Human-machine interface with control unit

All the physical items and their function on the control unit were described in section 6.6.1.1. The operator will utilize the controls and indicators on the control unit as follows:

Pre-start button (1.3)

The start button is an embedded red button that prevents the winch operator from accidentally activating the winch. This button is pressed to initiate a pre-start routine on the winch, followed by winch activation.

Signal button (1.2)

This button is a mushroom button and is used to signal to all signalling units similar to pulling a cable.

When the signal button is *not pressed*,

1. There is no voltage on the signal line;
2. All buzzers on all signalling units will be silent;

All display bezels will indicate a safe or unsafe condition and will display either green or red.

When the signal button is *pressed*,

1. There is a 24V voltage on the signal line;
2. All buzzers will sound (control and signalling unit);
3. All display bezels will not indicate as long as the button is pressed;
4. When the signal button is pressed for longer than 2 seconds, the winch will trip.

Status indicators (1.5 and 1.6)

The status indicators are two sets of 8 indicators that represent the status of each of the signalling units along the line(s). The following conditions are indicated:

1. Indicator permanently on - The corresponding signalling unit is active and functional;
2. Indicator(s) flashing - A signalling unit, or units at the indicated location may be faulty;
3. Indicator off - No signalling unit is attached at that location.

Control status (1.7)

There are 3 control indicators that indicate the status of the controller, the RS-485 communication lines, and the power status on the lines. More specifically, the indicators show the following conditions:

1. Left indicator steadily flashing - Control unit is good;
2. Left indicator off - Control unit powered down or faulty;
3. Centre indicator off - RS-485 communication is good;
4. Centre indicator on - RS-485 communication faulty;
5. Right indicator off - Power lines are good;
6. Right indicator on - Power lines or units are faulty.

Audible buzzer (1.4)

Each unit is equipped with a buzzer that sounds when a signal line is pulled. This buzzer emits sound at 105 dB over a distance of 30cms.

To prevent hearing impairment, units are installed so that users are not closer than 1 meter from the buzzer on the control unit.

Key reader (1.8)

Each control unit has a key reader that is used to control access to the unit, or to transfer logged system events onto a recording key.

Operator functions

Activate winch - An operator must activate a winch before it can be used. Without an access key - no access granted to the operator. Unsuccessful attempts are recorded;

Supervisor functions

Qualified personnel gain access to privileged functions on the control unit. These include:

1. Configure the system: When a new system is installed, or when the number of units on the system changes (new units are added or old units are permanently removed), the system determines its own physical configuration (the number of active units on lines 1 and 2);
2. Add or remove an operator: New operators are added in supervisor mode or operators are removed in this mode;
3. Upload event log: An internal event log is kept as an audit trail. This log can be uploaded to a master key and retrieved from a key at a later stage.

Interface 3 - Winch power supply and control interface

ESS power input: The ESS system operates on 32V AC or 550V AC depending on the requirement. As a standard, 32V AC is the required supply voltage.

ESS control output: A relay output is supplied to the winch control unit. This output presents the system state (safe / unsafe) to allow winch activation only in the unsafe state.

Interface 4 - Interconnection cable interface

Between a control unit and all the signal units, a standard 5-core reinforced cable is used. This cable carries electrical signals and supports mechanical “pull” signals. The cable is designed to withstand pull action.

1. A cable connection exists between a control unit and signaling units by means of reinforced cable sections of standard lengths;
2. A control unit is connected to signaling units on line 1 or line 2 of the system. Up to eight signaling units may be connected on each line by interconnecting the signaling units with standard cables;
3. The number of units on line 1 does not have to be the same as the number of units on line 2 as these two lines function independently.

Cable electrical characteristics

A basic overview of the cable connections is given below.

1. Output - 2 power lines (24V DC and 0V);
2. Bi-directional - RS-485 communications (+ and -);
3. Bi-directional - One 24V DC signal line.

Power lines (24V)

Each power line (left and right) can provide power of 24V DC at 1.5A. This is sufficient to power up to eight signalling units on a line. Voltage drops were taken into account in the design.

The power line is protected at the control unit against short circuits and “over current” conditions in cases where faulty components may cause unacceptably high current surges or constant overload conditions.

RS-485 lines

Industry standard RS-485 is used by the control unit to allocate addresses to signalling units. Communication takes place at 2400 baud.

Each signalling unit receives an address according to its position on the line during configuration. When a signalling unit is replaced, the new unit will acquire the same address as the faulty unit, addressing the need for modularity (“plug and operate”).

Lines 1 and 2 function independently and units are numbered from position 1 to position 8 on each of the lines. No termination is required on the communications line as the bit rate is low.

Signal line

A signal line is a single line that carries 0V when it is not activated and 24V DC when a cable is pulled. This signal line provides power to all signalling units when a cable is pulled and will power the buzzers and bezel indicators with this voltage.

This line functions independently from the communications line so that the signalling unit will fail to a physical state where the signalling function will remain as long as the cables are not damaged beyond functional capability.

Interface 5 and 6 - Human-machine interface with signalling unit / cable

All physical items and their functions on the signalling unit were described in section 6.6.1.1.

Since each cable also provides human communication capability by means of a “pull” action, the effect of a cable pull is provided.

When a cable is *not pulled*,

1. There is no voltage on the signal line;
2. All buzzers on all signalling units will be silent;
3. All display bezels will indicate a safe (green) or unsafe (red) condition.

When a cable is *pulled*,

1. There is a 24V DC on the signal line;
2. All buzzers will sound (control and signalling unit);
3. All display bezels will not indicate as long as the cable is pulled;
4. When a cable is pulled for longer than 2 seconds, the winch will trip.

6.6.1.3 System functional characteristics

Modes of operation

The ESS system has the following modes of operation:

1. **Initial reset mode**: When a system is first installed, or when a system is reconfigured, the system is in initial reset mode. This mode is automatically followed by supervisor mode;
2. **Supervisor mode**: Whenever a master key is presented to the control unit, the system will go into supervisor mode (see interface 3);
3. **Safe mode**: This is the system “idle” mode and the system is safe to use. The winch is disabled in this mode and signalling can take place. The bezel indicators on all components will be green. The control unit will indicate on the line status indicators which cable is signalling by indicating which pull switches are being pulled;
4. **Pre-start mode**: When a control unit has been activated and the start button on the control box has been pressed, the system will go into a 15s pre-start mode. The winch is disabled in this mode. Signalling can take place and the winch can be tripped in this mode. The bezel indicators on all components will be flashing red and green alternatively. Upon trip, the system will return to safe mode. The control unit will indicate on the line status indicators which cable is signalling by indicating which pull switches are being pulled;
5. **Unsafe mode**: After pre-start mode, the system will be in unsafe mode. The winch is enabled in this mode. Signalling can take place and the winch can be tripped in this mode. All bezel indicators will be red. Upon trip the system will go into trip mode. The control unit will indicate on the line status indicators which cable is signalling by indicating which pull switches are being pulled.
6. **Trip mode**: In trip mode the winch operator must reset the trip by presenting his / her key to the signalling unit on either side of the cable that was tripped. This will cause the system to fall back into safe mode. Signalling can still take place and the winch is disabled in this mode.

System failure modes

Different components of the system may fail during its lifetime. As a result, the following failure modes have been addressed, as discussed below:

1. **Short circuits between cable strands / connector pins**: This will cause (i) RS-485 communication to fail, (ii) high voltages over communication lines, (iii) high currents over supply lines, or (iv) signal line permanently on. The control unit can measure communication errors and high current conditions upon which the control unit will trip. Faults must be restored in cases where over-current conditions occur. The mine can specify whether the unit must remain in trip or should recover in cases where only communications is down since the signalling system operates on a separate circuit from the RS-485 communications;
2. **Open circuits of cable strands / connector pins**: This will cause communications to fail from a point onwards on a line. This will cause the control unit to trip. The control unit will attempt to restore the failure and production may proceed as long as signalling remains operational. A fault is logged. The mine can select his / her preference as this is configurable;
3. **Signalling unit failure**: Failure of a single box will not affect the system and indication is given on the control unit panel. Production can proceed and an event is logged for audit. The mine can specify if production should proceed when one unit fails;
4. **Control unit failure**: This is a catastrophic failure and will cause the winch to trip and remain in trip mode until replaced. Since the control box is a single point of failure, it is necessary to keep sufficient replacement / consignment stock of this component.

In most failure modes the system can recover as it can disable failed cables or signalling units (depending on where the fault occurred). The fail-to-safe level can be configured according to the requirement as it is possible to proceed with production when the signalling and trip functions (critical functions) are good.

6.6.1.4 System performance characteristics

Durability

Various factors influence durability, including use factors. However, components in the system were designed to provide durability in a number of ways:

1. The mechanical design was done to provide a robust enclosure from stainless steel;
2. Electronics were designed with operational margins of more than 100% on input and output protection - all electrical inputs and outputs are protected against over-voltage and over-current conditions;
3. A fail-to-safe design was followed on the critical functions such as signalling and tripping.

Health and safety

Audio at 3kHz is emitted from the unit during signalling. Exposure to high levels of audio noise may lead to hearing impairment. As a result, the total number of hours over which the unit may be used when continuously emitting sound (at a distance of no less than 1 meter from any box) should be kept to less than 2 hours.

Maintainability

A swap-out policy was followed for unscheduled maintenance. The following specific guidelines should be followed:

1. No component should be opened for second-line repairs on the premises of the client;
2. The swap-out policy was designed into the system and facilitates a “drop-in” replacement of signalling units and control boxes (control boxes must be reconfigured in terms of allowed operators);
3. Re-use of components (signalling units and cables can be used anywhere) facilitates a reduced consignment stock burden and simplifies repair;
4. Online diagnostics indicate cable faults and signalling unit faults to reduce system down time;
5. Faulty units may be repaired in a follow-up shift and the system can maintain production (signalling and tripping will still work with faulty units);
6. All fault conditions and events are logged to identify recurring fault conditions or user action.

EMC

Although no formal EMC requirement exists for the mining environment, the system was designed to function under severe electro-magnetic conditions through the following:

1. Use of communication methods with high common-mode rejection ratios or high margins;
2. EMC protection on all inputs and outputs, specifically electro-static discharge as well as galvanic isolation;
3. Components in the system were designed not to radiate.

Transportability

Signalling units will be most exposed to harsh conditions and were designed with the following requirements:

1. Humans will carry the signalling units. Therefore a carry handle was added to the box as a standard;
2. Control units and signalling units are transported in protective boxes and are protected against shock and vibration.

Materials processes and parts

All materials used in the design were selected to withstand harsh underground conditions. More specifically, the following are important considerations:

1. Enclosures are manufactured from 3CR-12 stainless steel and powder coated to withstand all environmental conditions common to mines;
2. Connectors;
3. Cable material;
4. Exposed grommets and seals.

Modularity

All units were designed to be modular and interchangeable. This is to facilitate swap out and replacement on site as well as to reduce the skills level requirements on maintenance personnel in operation.

The following considerations were taken into account:

1. All units use the same standard plugs and sockets, are modular and can thus be replaced when damaged;

2. In new installations, a control unit will follow a registration routine to find all the signalling units that are connected to the control unit;
3. Each signalling unit is assigned a number according to its position along the line. This means that, as one walks down the gully, one can assign a location according to the position of the signalling unit along a line;
4. Signaling units can be interchanged and will not lose their location information on a line. That is, when a faulty box is replaced, the new box automatically reconfigures itself and becomes a “drop-in” replacement of the faulty signaling unit;
5. A faulty control unit can be replaced with a functional unit, but needs to be reconfigured to determine the system configuration;
6. Any functional cable can replace a faulty cable.

Safety

The system controls the safety of miners and winch operators. Although all possible steps were taken from a design point of view, the following aspects are of extremely high importance:

1. Operational inspection procedures must be put in place to consider a catastrophic failure (for instance, when a control unit fails);
2. Procedures must be put in place to test for explosive gasses before any system is powered up, and to provide adequate ventilation when operations proceed;
3. Failure modes were considered extensively during the development of the product and all known failure modes are documented. These must be communicated to personnel and procedures implemented.

Human performance engineering

In light of the system being a communications and safety system, the following design criteria were followed:

1. All human interfaces are clear in terms of its use;
2. Visible and audible signalling was designed to cover normal view angles;
3. The number of interface controls were kept to a minimum;
4. Maintenance is kept to minimum requirement levels.

Standards of manufacture

The following specific requirements are addressed:

1. All electronic sub-assemblies are manufactured in an ISO-9000 facility;
2. All enclosures are manufactured to manufacturing specification;
3. All pull cable is manufactured to specification NCB 643/1979;
4. All plugs and sockets are manufactured to IEC 309 standard.

6.6.1.5 Product risk assessment

The product risk assessment performed on the ESS system is presented in Appendix A. This product risk assessment is done in the matrix format, and consists of a component and material assessment, the risk assessment matrix, considered risk cases, product risk analysis table, risk mitigation, and explanation of hotspots.

6.6.2 Electronic signalling system 2 (ESS2) development

Equipment of the electronic signalling system 2 is presented in this section. This system (ESS2) has been determined by means of risk-reduction using the ESS as a reference. In the risk-reduction process high-risk activities were identified and adjusted for an alternative solution. The ESS2 system definition was defined in the preliminary design in the ABR process as discussed in Section 6.5.9.1. Only functions were changed in the trade-off and the system interface definitions of the ESS2 are the same as for the ESS.

Because no substantial interfaces were changed (in terms of its use), the same electronic hardware of the ESS could be used to implement the ESS2. Functional changes were done by firmware updates to both the control unit and signalling units.

6.6.2.1 System configuration (ESS2)

In the implementation of the ESS2, smaller enclosures were used and a different plug configuration was employed (these were minor changes) – these components are discussed in this section.

The control unit and signalling units are described below (the signal cable used is still the same as presented in Figure 72). A custom key was also developed to withstand corrosive environments.

- Remove Activity 13: The firmware of the control unit and signalling unit was updated to remove Activity 13 as proposed from the simulation results performed in the trade-off. This means that when a trip is initiated from the gulley, the system can be reset at the control unit and the winch driver is not forced to walk / crawl to a tripped signalling unit for a reset. As a result, the access key reader on the signalling unit was removed;
- Automate Activity 12: A fixed time delay is enforced, when the system has been tripped along the gulley, to allow the miner to safely cross the gulley before scraping operations can proceed. This function is automated as defined by the ABR analysis, and forces the winch operator to wait before the winch can be started again;
- Enclosures: The size of the enclosures was reduced to allow for smaller enclosures with a different plug configurations;
- Reduce signalling unit's bezels and buzzers: Upon installation of the ESS, it was found that one bezel and buzzer provides sufficient status indication as the signalling units are spaced fairly closely on both sides of the gulley. The design of the LED bezel is as such that it is visible at a 90 degree viewing angle. Therefore the ESS2 system uses one bezel and buzzer;
- Access key: A custom access key has been developed as the commercial off-the-shelf key used during the ESS proved not to withstand the harsh underground environments. This access key was specifically developed for a highly corrosive environment. Although the access key is not required to reset signalling units when tripped, the key is still used by the winch driver for identification and audit purposes on the control unit;
- Interconnection cable: The same interconnection cable and mechanisms are used as presented for the ESS.

The control unit, signalling unit and access key developed for the ESS2 system are shown in the images on the next page.

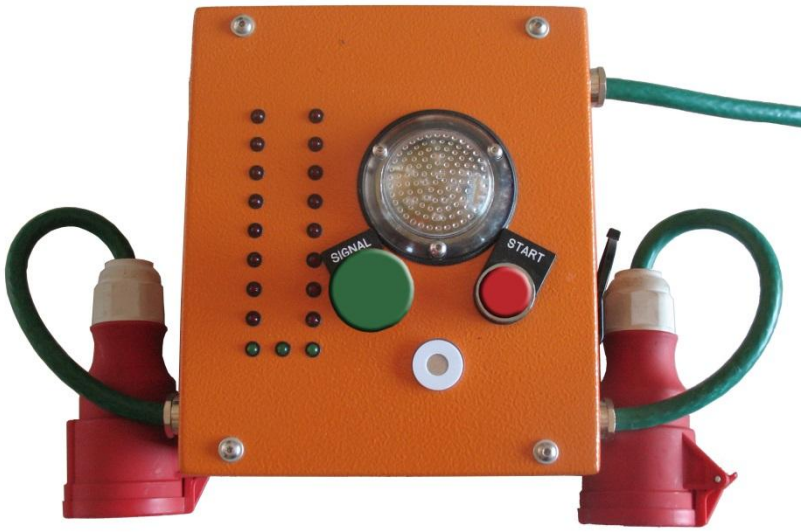


Figure 74 : ESS2 control unit

Figure 75 : ESS2 signalling unit

Figure 76: Access key for ESS2

6.6.3 Electronic signalling system 3 (ESS3) development

The focus of the electronic signalling system 3 (ESS3) was to develop a lower cost solution. The definition of the ESS3 was derived from the risk-reduced ESS2 model. To reduce the cost of the system, functions and features (hence, system components) must be reduced, causing a change in architecture / configuration. In the definition the ESS3 system presented in Section 6.5.9.4, the new system architecture and layout were shown. Here, the number of signalling units is reduced so that only a control unit and one signalling unit remain. The signalling unit is used to allow for signalling on both sides of the gulley, while status indication is presented by both units, located at the winch.

Limited system state indication is used along the gulley with the ESS3 as status indication is only available at the winch itself. Although the same hardware and circuits presented in the ESS and ESS2 could be used for this configuration, a completely new system was developed to further reduce cost on a sub-component level. This cost-reduced solution (ESS3) is presented in this section.

6.6.3.1 System configuration (ESS3)

In the system development, system components were redesigned and reduced in quantity as described below:

- Enclosures: A new low-cost enclosure was designed for the control unit and signalling unit. Plastic material was used for this design which is not as robust as the metal enclosure, but as the system is only located at the winch, limited shock from blasting is experienced;
- Non-intelligent signalling unit: The signalling unit was developed to only replicate the status indication of the control unit and to provide a signalling function. In the design of the ESS and ESS2 the RS485 communication standard was followed as signals and unit status needed to be communicated to the control unit – this was removed;
- Control unit: New electronic hardware and firmware were developed for the control unit. Only the necessary circuits were implemented adding to the cost saving. As no serial communication was required due to the simplicity of the signalling unit the communication circuit could be removed. Further, the access key reader was no longer required as access keys are not present on this device. There is also no status display on the unit because no signalling

units need to be presented along the gulley. This simplified circuit results in the use of simplified processors and a reduced circuit configuration;

- Interconnection cable: A 5-core interconnection cable is used between the control unit and signalling unit. As both these units are located at the winch, this cable is short;
- Pull cable: Instead of the electrical pull cable used in the ESS and ESS2, a strain wire is connected to a device (signalling or control unit) on both sides of the gulley for signalling purposes;
- Winch controller interface: The same interface to the winch control unit is implemented for all electronic systems.

Both the control unit and signalling unit for the ESS3 configuration are shown in Figure 77, together with the interconnection cable.

Figure 77 : ESS3 Control unit (left) and signalling unit (right)

The internal configuration and developed circuit board for the control unit of the ESS3 are shown in Figure 78 on the next page. No circuit board is present at the signalling unit, as the bezel, buzzer, and pull switch are directly connected via a 5 core interconnection cable.

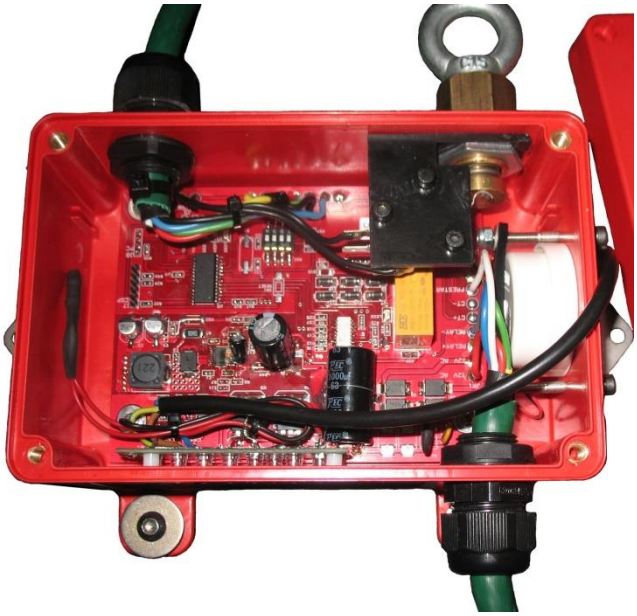


Figure 78 : Control unit circuit board mounted in enclosure (ESS3)

6.7 System cost comparison

Relative equipment costs of all signalling systems are presented in this section. Although the winch signalling system is designed to reduce risk, it cannot be done at all cost and a relative comparison will provide decision support information to mines.

A cost comparison between the solutions available is presented in Table 34. This cost comparison is normalised where the electronic safety system cost is presented relative to the conventional air whistle system (AWS). Note that installation effort was not included in this comparison.

Table 34: Normalised signalling system cost comparison

Winch signalling system solution	Normalised cost	Notes:
AWS (Conventional system – AS-IS)	1	Single unit located at winch controller with strain wire used for signal cable.
ESS (Initially proposed system)	7.4	Configuration: One control unit, 4 signalling units, 4 pull / interconnection cable (no access keys)
ESS2 (Risk-reduced system)	7	Configuration: One control unit, 4 signalling units, 4 pull / interconnection cable (no access keys).
ESS3 (Cost-reduced system)	2.3	Configuration: One control unit and one signalling unit with strain wire used for signal (pull) cable.

The results from Table 34 show high costs for the ESS and ESS2 systems and a significantly reduced cost for the ESS3.

Note that the costs for the ESS and ESS2 differ from one installation to another as more signalling units and interconnection cables are required for longer gulleys which add to the cost of the system.

With the system cost available, the following options exist:

- Implement a more expensive, risk-reduced solution (ESS2 - lowest risk option);
- Implement a medium-risk, low cost solution and apply savings on human performance in terms of additional training and control.

The decision above was left to the mine, with the result that the higher cost systems (ESS2) were applied in long centre gulleys in order to provide sufficient signalling and indication along the gulley, as per regulation. The lower cost systems (ESS3) were used in strike gulleys where mono-winches were used and gulleys were shorter so that sufficient signalling and indication were still effective.

In this case study, cost comparisons were done after equipment had been developed. These costs must be estimated before detail design and development commences. This will allow the mine to select a system in the preliminary design phase as the focus of the ABR approach is to develop the correct technology from the start.

6.8 System utilization

The three systems developed as part of this case study were evaluated by the mines. Feedback from mining operations and acceptance by mine management was used to validate the resulting artefacts, and hence (at least, in part) the effectiveness of an ABR acquisition process.

6.8.1 ESS utilization

The ESS system was the first system evaluated in mining operations by following the mine's safety policies (it is by no means allowed to "experiment" on humans in operation and mines have processes in place to first evaluate safety systems in controlled environments). This system consists of the full function set as defined in

the functional analysis in Section 6.4.2. This system was not accepted by mining operations and the following observations were made during evaluation:

- The system was not effective due to production losses (as a result of activity 13) and it was highly probable that malicious damage and bypassing of the system would result;
- Costs were prohibitive, and combined with a loss in production, the ESS did not provide a final solution.

The findings provided sufficient evidence that the ESS system was not accepted by mining operations.

6.8.2 ESS2 utilization

The risk-reduced system (ESS2) was implemented in the same test environment as the ESS. This system definition was given in Section 6.5.9.1. Feedback from mining operations was positive and production impact was lower with very little risk of equipment being maliciously damaged or bypassed. As a result, the system was accepted by the mine and more than 2000 systems with the ESS2 configuration have been installed in South African mines. These systems are being installed in long gulleys as the status of the system is visible when using signalling boxes (confirmed by analyses).

6.8.3 ESS3 Utilization

The cost-reduced system (ESS3) was implemented in the same test environment as the ESS2. This solution was also accepted, with positive feedback from mining operations.

More than 4500 systems (ESS3) have been installed in South African mines. This ESS3 configuration is typically used in shorter gulleys, such as strike gulleys, where the winch is visible from the gulley. In the longer gulleys, the ESS2 system is deployed.

6.9 Case study overview and discussion

The ABR process was applied to the acquisition of an electronic safety system (ESS) for scraper winch operations in order to replace conventional air whistle systems (AWS). All steps of the ABR process were applied, with results from each step shown and discussed in detail in the sections above.

The existing system (AWS) was analysed to form a comprehensive understanding of the current system and its operations, with the focus to implement this solution in a simulation model. This is of importance as the operational parameters and risk-related factors for the AS-IS design were required for a consistent and representative model. The TO-BE system was defined by a local mining group, with all required functions and desirable characteristics provided by the mine. This set of requirements was defined by the mine following a traditional approach to acquisition and risk management, as discussed in the problem statement (Chapter 3). This candidate system was defined as the electronic signalling system (ESS) on which a detailed analysis was performed (both the AS-IS and TO-BE systems were analysed in depth). This analysis is of major importance as the system was analysed in an operational context, taking all functions, resources and interfaces into account. The analysis was done by doing a functional analysis for each system, where complete behavioural models and resource allocations were defined as outputs. The resource allocation showed all resources and their interdependencies with respect to system activities / tasks. Risk-related information was determined from the resource allocation in terms of resource failures and affected activities.

Once the functional analysis had been performed, a full understanding of the technology and operations was gained. This allowed the construction of a realistic simulation model representing candidate systems in operation. A generic operational model was constructed in SIMIO, where the full function set of each system (AWS and ESS) was implemented. Possible actions taken by human operators and miners interacting with the system were added to the model. This was done by using risk scores allocated to human resources. The risk score represented the level of risk (from 1 – 5) of all human resources. Risk levels were used to set up volatility tables representing the probabilities of actions followed by human resources. Variability was allowed where human tasks were performed by using stochastic modelling, as the processing time of tasks and decisions differed between operators.

The simulation model was evaluated in terms of risk-related response factors. A hazardous exposure factor (HEF) and a production loss factor (PLF) were defined

directly relating to hazardous exposure time and production loss time. Different scenarios were set up in the simulation, representing the combinations of the resource risk levels – a total of 25 scenarios resulted. It was found that for 200 simulation runs a maximum mean confidence interval of 6% of the output response range was determined at a confidence level of 95%. The averaged results (risk-related response parameters) from the 200 simulation runs (for each scenario) were used to compare candidate systems' risk-related response factors as a function of human variability / risk scores. These risk-related factors were graphically compared and were given in Figure 46 and Figure 47.

Results indicated high hazardous exposure for the AWS (when compared to the ESS), while the ESS showed high production loss (when compared to the AWS). This information showed that, although the ESS provided a safer operational environment, production loss was significant.

The ESS system was further analysed to identify high-risk activities. This was done by setting up a simulation model where deviations were introduced into all activities. These deviations were in the form of minimum and maximum activity times and failures of activities due to resource failures (from the resource allocation table and functional grouping). The impact on risk-related factors (HEF and PLF) was determined for each activity. These impacts were summarised in Table 32, indicating high-risk activities of operations (including equipment and human failure).

When individual activities were analysed, an additional risk factor was identified in a transitional activity and was added to the initial risk-related response factors of the system. This risk-related factor was defined as a prestart-related hazardous exposure factor (PHEF) and indicated the number of miners (out of a 100) inside a gulley when the winch was started. The prestart activity was found to be a transitional activity (safe-to-unsafe transition) which deserved additional attention.

The activity-based risk process indicated that risk factors could be reduced by addressing activity 13 and activity 12. The result was that the function of resetting the system at a signalling unit along the gulley (after a trip) was removed. In addition, a fixed hold-off time was implemented, after a system had been tripped from a gulley, to allow miners to cross the gulley safely before proceeding with scraping. This system was defined as the ESS2.

The simulation model was updated with the functions as proposed for the ESS2. The results from the ESS2 were compared with results from AWS and ESS simulations, and showed a significant improvement in the production loss (PLF) with respect to

the ESS production loss factor – this was confirmed by the mine. The risk-reduced system (ESS2) showed similar low risk factors for production loss of the AWS system, while the safety risk of the ESS2 in terms of hazardous exposure was similar to the low risk of the ESS (the ESS2 showed a higher HEF than for the ESS due to the additional production time that resulted). The PHEF was also significantly reduced for the ESS2, where the PHEF was high for the AWS. Comparisons of risk-related factors between the three systems were shown in Figure 61 to Figure 63.

Once the risk reduced system (ESS2) had been determined from the activity-based risk process, the system was further analysed with a focus on reducing equipment cost of the system. It was accepted that cost reduction would limit functionality of the system and would therefore add to risk, but the relative impact of these changes was important and was determined using simulations. The cost-reduced system was defined by altering the system configuration (reduced configuration) and used a control unit at the winch with a single signalling unit to allow for signalling from both sides of the gulley. This system configuration resulted in interface changes and, therefore, new volatility tables were constructed and implemented in an updated simulation model. The evaluation of risk factors for the ESS3 showed an increase in hazardous exposure, but still significantly lower than the high HEF of the AWS. The PLF and PHEF for this solution were similar to the ESS2. The relativistic comparison for the ESS3 solution was presented in Figure 66 and Figure 67.

All three systems were developed and evaluated in controlled environments. The ESS system was implemented first (as this was the system requested by the mine) but was rejected by mining operations. This was due to production loss of the system, potentially resulting in bypassed and maliciously damaged systems in operations. Both the ESS2 and ESS3 systems were accepted by the mine, with a significant number of systems currently in use at South African mines.

A cost comparison showed the cost normalised relative to the conventional AWS system. The cost of the ESS is 7.4 times higher than the AWS, while the ESS costs 7 times more than the AWS. The cost-reduced solution (ESS3) cost approximately 2.3 times more than the AWS.

The results from the ABR analysis allow mines to select a system (ESS2 or ESS3) based on cost and risk-related factors for candidate systems. The risk-related factors are not only determined in isolation for equipment, interfaces, or failure analysis of individual components, but for the combination of equipment and human variability in operations (thus, sensitivity of systems with respect to human variability and resource

failure). This information assists in selecting a system that addresses safety risk by taking into account human factors as part of the overall system effectiveness. Safety risk associated with electronic safety equipment could thus be reduced at a resource level by addressing human factors.

In this case study, the results indicated a reduced HEF for the ESS3 system when a MCRL3 (miner crossing gulley, risk level 3) was used, compared to the HEF of the ESS2 system for the same resource combination. Given this information, the mine can select the low-cost ESS3 system and invest in human resources to decrease associated risk levels. If this risk is not acceptable, risk can be further reduced by investing in both technology (ESS2) and the human resources at organisational level.

In the simulation results of all the winch signalling systems, the sensitivity of a system with respect to human resource combinations was determined. The results showed that the ESS systems were sensitive to change in risk levels of miners crossing the gulley, with a reduced sensitivity for the risk level of a winch driver. This means that the focus should be to manage risk levels of miners crossing a gulley as opposed to a primary focus on risk levels of winch drivers. In order to achieve this, the interface between miners and equipment (along the gulley) must be ergonomically sound.

In the requirements for the ESS system (as provided by the mine), the use of an access key was initially specified to manage winch drivers' identities and accountabilities. This means that risk levels of winch drivers were managed as the equipment forced the driver to perform specified tasks, such as resetting the system in the gulley. This requirement was effectively challenged as a result of following the ABR process.

The ABR analysis results clearly show that, for the ESS2, primary safety functions were performed by the signalling system itself, without compromising production, and the focus should be on awareness and correct use of the electronic winch signalling system by miners.

Thus, although the winch drivers should still be managed by the equipment, the focus should be on providing reliable equipment as well as training and awareness of miners that interact with that equipment.

6.10 Summary

The application of an activity-based risk (ABR) acquisition process was presented in this chapter. Results showed that the ABR process, specifically for the winch signalling systems, provided the following benefits:

1. **Quantification:** At the onset of the research, a specification was provided by a mining group for the proposed system (ESS). Although it became evident that a production loss using this system could result (due to Activity 13 – reset system along the gulley), this loss could not be quantified. The operational simulation modelling introduced by the ABR process allowed for relativistic comparison of risk-related factors, and showed a significant increase in production risk for the ESS system when compared to the AWS system. This was confirmed during the development and implementation of the ESS solution as evaluated by the mine in a controlled environment. Risk-related factors that were identified include hazardous exposure as a factor (HEF) a, production loss as a factor (PLF), and later also a prestart-related hazardous exposure factor (PHEF);
2. **Identification of high risk activities:** After the risk of a concept system had been determined (in terms of risk-related factors), high risk activities were identified by means of introducing deviations and failures for each activity. The system model was analysed to determine sensitivity of the system's risk-related factors with respect to deviations. In the case study, the analysis of each activity showed the impact of activity failures as summarised in Table 32. Transitional activities were identified as specifically important and are discussed in the following list item;
3. **Transitional activities:** In the risk analysis of individual activities, it was observed that the HEF for the prestart activity (Activity 4) was not particularly high. However, since activity 4 was identified as a transitional activity, further analysis was required. From the analysis, it followed that safety risk should also be expressed in terms of the number of occurrences when a miner was inside the gulley when the winch was started, bringing into consideration the increased impact of a failure event in a transitional activity. Such a failure event posed a higher safety risk compared to instances where the gulley was entered with the winch running. A "prestart-related hazardous exposure" value was defined, which indicated the number of occurrences when the winch had been started with a miner in the gulley. This risk factor was used to clearly highlight the significant impact of a transitional activity – in this case, the prestart activity. This factor was

added to the evaluation of the systems and all its activities. This factor would not have been identified had activities not been analysed individually for sensitivity.

4. **Risk-reduction:** The analysis of sensitivities for each activity allowed designers to introduce mitigating functions to define a risk-reduced system. In the case study above, the risk-reduced system was defined by altering Activity 12 (hold-off time to clear the gulley after a trip) and Activity 13 (investigate the trip condition). Activity 13 caused a loss in production, which increased the probability of malicious damage and bypassing. Production loss may have been obvious from a functional analysis, but its relative impact was not known as it was not possible to quantify relative losses without following an ABR approach. ABR allowed the designers to compare losses and to adjust system and equipment functionality accordingly. The effect of Activity 12 was not initially obvious when considered in isolation, but was identified as being a critical function during ABR analysis. Quantification allowed designers to compare risks relativistically, where results for the ESS2 showed significant improvement over the high risk factors of the initial ESS system. Both activities were analysed using simulations following a functional analysis. This ensured an integrated approach that balanced safety and productivity.
5. **Cost reduction:** Cost reduction was done in the case study by reducing the physical component count and complexity of the system. As interfaces have changed in the new configuration, new volatility tables were set up representing the probabilities of failures or deviations relating to human risk levels. The risk factors were evaluated for this low cost system (ESS3) and showed an increase in hazardous exposure when compared to the ESS2 system, but were still significantly lower than for the ESS system.
6. **Human resource variability:** The ABR process showed the sensitivity of risk-related factors with respect to human performance variability. This was determined by allocating risk scores (resulting in volatility tables) to all human resources. The sensitivities were visualised in the analysis of each candidate system. This information shifted focus from a hazard-based risk analysis of technology towards analysis of equipment including human resources. In the case study it became evident that the system hazardous exposure was more sensitive with respect to performance variability of miners interacting with the system (crossing the gulley) than to performance variability of the winch driver. With this information, the use of access keys used by winch drivers was reconsidered and eventually removed;

7. **Relativistic comparison:** It is important to use the same input parameters and assumptions when constructing the operational model for simulation, as was done in the analysis of the winch signalling system above. The relativistic comparison showed that the AWS did not perform safety-wise, but supported productivity. The ESS limited production to an unacceptably low level, but increased safety significantly. The most successful system was obtained by removing production limiting functionality and retaining safety critical functionality. The end result was obtained by using simulations that simplified the process as only functional adjustments (with minor architectural changes) had to be implemented with respect to the reference model.
8. **Modelling, simulation and visualisation:** The generic simulation model was implemented in the SIMIO visual simulation package. This allowed designers and stakeholders to visually inspect actions of human resources and equipment states in operation. This graphical representation assisted with the communication of risks and to gain information from operations.

In conclusion, the ABR acquisition process provided a risk perspective on the development of winch signalling equipment and assisted significantly in the definition of a function set for the final winch signalling system. Simulations and operational verification showed that two systems were required, a risk-reduced and cost-reduced system. The risk-reduced system is preferred in long gulleys for its communication ability, while the cost-reduced system is used in volume in short gulleys. It may be the case that an intermediate solution exists to provide a further balance between risk and cost, but this was not verified in practice.

As a model was constructed and no “experimentation” was done in operation, the development phase did not increase the risk of hazardous exposure as adjustments could be made on an abstracted model. Finally, the operational model assisted significantly in the development of an acceptable solution and allows future candidate systems to be compared to the current electronic signalling system.

Chapter 7
Conclusion

7.1 Introduction

This chapter provides an overview and conclusions of this research. An overview of the research is presented, followed by results and contributions of the ABR process. Finally, validation and verification of the study are presented, followed by suggested future research.

7.2 Research overview

This research study was focused on the acquisition of electronic safety equipment for mines. The research was conducted within the framework of design science research (DSR), to ensure that a structured research process was followed. The research, in context of the DSR framework was presented in Chapter 2.

The existing acquisition process and risk management methods used in the SA mining environment were analysed by means of observations, case studies, risk documentation and literature. It was evident from this analysis that shortfalls exist between the acquisition and operations phases in terms of the management of risk from a full life cycle perspective. The specific research challenges were discussed in Chapter 3.

A literature study was conducted (Chapter 4) to find relevant literature to the research challenges from a combination of engineering fields. The focus areas in this literature study include risk definition and terminologies, a risk management framework, risk analysis methodologies and characterization, existing risk assessment tools and techniques, human error and operational modelling, and systems engineering. The research showed that a gap was still evident between the acquisition and operational phases of the system life cycle. Valuable information was obtained from literature, as all research challenges were translated to research solutions in Chapter 4.

The discontinuity between the acquisition and operational phases (engineering and mining) was addressed in this research by an activity-based risk (ABR) acquisition process presented in Chapter 5. Activity-based risk forms part of the preliminary

design of the product's full life cycle. Preliminary design is the primary focus of the ABR acquisition process, making the AB process a "middle-out" process as opposed to top-down or bottom-up processes. The focus of the ABR process is to find the set of functions that gives acceptably low risk. The sensitivity of risk-related factors is determined with respect to human performance variability in operations. This enables a designer to find a balanced (between productivity and safety), cost-effective solution in a relativistic sense.

The ABR process was introduced in a real-world case study. In this case study an electronic safety system was developed to address the safety risks in winch scraping activities. The existing air whistle system (AWS) was analysed in the ABR context together with the proposed electronic signalling system (ESS) from the mine. Risk-related factors were defined in terms of production loss time and hazardous exposure time. It was evident that, although the safety risk factor was reduced significantly by the ESS, a significant increase in the production risk factor resulted when comparing the ESS and AWS. The ABR method was employed to determine high risk activities for all candidate systems, resulting in the definition of a new system (ESS2) where the production risk was significantly decreased. A cost-reduced system (ESS3) was evaluated, and showed an increase in hazardous exposure with respect to the ESS2 when used in long gulleys, but the cost was reduced to approximately 30% of the ESS2. All three systems were developed and evaluated in controlled environments. Feedback obtained from mines correlates with the ABR model results, and validates the operational models (SIMIO models), and adds to validation of the ABR process. Detailed steps of the analysis, operational simulation model (SIMIO), human variability modelling, risk-related factor definitions, model evaluations and results, activity risk contributions, trade-off results, and summaries for the ESS physical equipment were presented in chapter 6.

7.3 Results and contributions of the ABR acquisition process

The ABR acquisition process was defined to support mines and system developers with the acquisition of electronic safety equipment. ABR compares electronic safety equipment on a relativistic basis using risk-related factors as performance measures. This process was defined in Chapter 5, Section 5.3 as shown in Figure 21. The ABR process combines systems engineering principles, risk analysis principles, and safety principles to provide a single framework that addresses all requirements as defined in the research problem.

7.3.1 Contributions

The ABR acquisition process is characterised by the following benefits:

1. **Quantification:** The ABR method uses risk-related factors to assist in trade-off analysis. Risk quantification is required to enable a designer (and client) to perform a relativistic comparison of equipment effectiveness when used in an operational environment. Risk definitions are specific to an ontology, and the strict definition of risk cannot be applied in any environment without care. Therefore, to simplify communication with mining operations and engineering, it is necessary to define operational equivalents of risk factors, called risk-related factors. These factors, although not strictly defined as risk factors, are used to indicate hazardous exposure and production loss and are used to compare different equipment options. In this regard, the translation allows quantification in the mining operations ontology, and allows comparison and simplified communication between the mine and system analysts.
2. **Identification of high risk activities:** High-risk activities must be identified and managed to correctly address risk – the ABR method allows the designer to identify high-risk activities in an integrated way. Activities logically combine low-level tasks and resources in order to assess risk in an integrated manner. Activity-based risk analysis expands on the concept of baseline risk – high-level physical locations and activities that pose high risk as defined by SIMRAC – by providing more granularity at lower levels of operations. Activities are thus identified at operational level following a functional (behavioural and architectural) analysis. Activity-based risk analysis provides an integrated (systems) view and implements a complex cause-effect relationship (similar to a Fishbone analysis, but wholly integrated) that is analysed for the whole system model for all introduced deviations, and not a single event path alone. This kind of analysis cannot be done for complex systems without the use of a simulation tool.
3. **Transitional activities:** ABR allows transitional activities to be defined and treated as high risk contributors by default. Transitional activities introduce additional risk since systems change from safe to unsafe states. Communication between equipment and humans (i.e. ergonomics of the human-machine interface) improves awareness of states and is critical in transitional activities (equivalently, states in a simulation model). It is, therefore, imperative to analyse transitional activities extensively with specific attention to impact of failures in these activities.

4. **Risk-reduction:** ABR allows a systematic reduction in risk as it allows focus on specific activities in a sequential way, which speeds up design and increases understanding of risk. Electronic safety equipment for mines is typically designed to control operational states (the safety environment) and to automate functions by allocating safety-critical functions to equipment as opposed to humans. In the process of design, a functional analysis is used to clearly show all tasks at equipment and operator level in a system context (an integrated view). High risk may also be present in cases where functions are used that cause production loss. Functions that cause production loss must be identified and adjusted or removed to provide equipment with minimum impact on productivity and maximum impact on safety. Safety functions may have to be added to, or removed from the initial concept after analysis. Such functions may appear to be insignificant at first, but could have significant impact on safety. This form of "optimization" can only be achieved by using a focussed, systems approach as provided by the ABR acquisition process.
5. **Cost reduction:** Similar to risk reduction, ABR provides a means for reducing cost by adjusting or removing activities, equipment functionality, and resources as required. There are different operational environments in deep mining operations and one solution will not fit all operational requirements, meaning that a feature rich system may not be the most cost-effective solution for smaller installations. An important consideration is thus equipment cost, as safety equipment is considered a non-productive capital expense. It is imperative to perform a comprehensive analysis in order to fully understand the effects of functional reduction. This becomes possible when performing a relativistic comparison of systems in an integrated manner – the side effects of functional and resource reduction must be considered system wide. The balance between risk and cost is found when the subset of critical functions has been identified and performance quantified.
6. **Human resource variability:** ABR allows human variability to be modelled and integrated with the system in an operational environment. Human resource failure is a reality that must be addressed when designing safety systems. Human performance variability runs in parallel with failure and affects system performance in complex ways. Performance variability can be introduced by considering variability in all decisions and actions taken by humans in the system (as opposed to an isolated operator-machine approach). This form of sensitivity analysis starts with a functional analysis (resulting in event tree analysis, resource behavioural modelling, resource allocation, architectural function and

interface analysis, and state modelling) followed by the definition of volatility tables for human resources linked to risk scores. Equipment options can thus be compared when different candidate systems are operating in an integrated system that includes human performance variability.

7. **Relativistic comparison:** Equipment effectiveness can be compared in a relativistic manner to find an optimal solution by using ABR. In order to perform a relativistic comparison, a reference model must be available. The current (AS-IS) and conceptual systems (TO-BE) provide baseline functionality for comparison, with the current system used as reference. When the ABR process is followed, risk-related performance measures (factors) are used to measure effectiveness on a relativistic basis, comparing different candidate systems in the same operational environment, using the same resources. By following a relativistic approach, environmental assumptions common to all candidate systems should not affect differential results.
8. **Modelling, simulation and visualisation:** ABR uses operational simulation to address complexity. A key factor to the success of a system is the ability to communicate value of a solution to decision makers in management. Simulation provides decision support information, allows visualisation of performance, and supports communication between designer and client. More specifically, management is usually more interested in high-level results, while operational personnel are more interested in contributing to the model and understanding the impact of decisions at operational level. The model and simulations provide a mechanism to facilitate cooperation and understanding, which results in a more complete and accurate system configuration. Finally, an operationally consistent model assists in future risk reviews by providing a baseline for future reference.

7.3.2 DSR artefacts

The design science research process produces artefacts in more than one form; in this research, the following artefacts resulted:

1. **Knowledge base:**
    a. The main contribution to the knowledge base is the principle of activity-based risk analysis that includes human performance variability in the modelling and definition of safety equipment;
    b. Inclusion of the ABR method in the preliminary design phase of systems engineering resulted in an integrated ABR acquisition process based on risk;

c. An operational model (SIMIO) for scraper winch operations also adds to the knowledge base and can be used in future development;
d. The documented case study on scraper winch operations shows how the ABR method can be used to perform relativistic performance comparison in practice.

2. **Developed artefacts:**
    a. In the context of design science research, the artefacts include the ABR method and acquisition process that have been subjected to a rigorous verification process;
    b. Two successful signalling systems resulted from this research. These are currently being used in mining operations.

7.4 Verification and validation

Verification and validation are key elements of the design science research process. The “forward” process was followed, during which abstractions were made of the real world problem. An activity-based risk acquisition process was defined and documented. A “reverse” process was also followed, where the acquisition process was evaluated as part of a real-world case study. In the section that follows, the validation of the research problem, research solution and ABR process model (one of the artefacts) are presented in a traceability matrix as shown in Table 35 (on the next page), after which the matrix is further discussed.

Table 35: Research verification and validation

	Information sources / Research challenges	Detail requirements are not defined	Sub-optimal safety technology often implemented	Focus is on hazardous exposure	Lack of integration and limited full life cycle perspective	The focus of risk assess-ments is mainly expert input and hazard based	Reactive incident risk management approach is followed	Impact of specific tech-nology is not measured using a common norm	Lack of human integration in risk assessment
Chapter 3	1. Mine Health and Safety Act	↓		↓		↓	↓	↓	↓
	2. SIMRAC Documentation	↓		↓		↓	↓	↓	↓
	3. Mining Documentation	↓		↓		↓	↓	↓	↓
	4. Observations during Case Studies	↓	↓	↓	↓	↓	↓	↓	↓
Chapter 4	**Literature focus areas / Research challenges**								
	1. Risk definition and terminology				↑	↑		↑	
	2. The risk management framework		↑	↑	↑ ↓		↑	↑	↑
	3. Risk analysis methodologies and characterization	↑	↑		↑	↑	↑	↑	↑
	4. Existing risk assessment tools and techniques	↑	↑ ↓	↑ ↓	↑ ↓	↑	↑ ↓	↑	↑ ↓
	5. Human error and operational modelling					↓	↓	↓	↑ ↓
	6. Systems engineering	↑ ↓	↑	↑	↑ ↓	↓	↓		↓
Chapters 5 and 6	**Literature focus areas / Research solutions**	Define detail system requirements in preliminary design	Follow an integrated approach	Follow a balanced app-roach (production, tech-nology, safety, usability)	Follow an integrated SE approach	Use functional analysis during preliminary design to obtain all relevant information	Follow a proactive risk management approach	Follow a relativistic approach when comparing technologies	Introduce resource risk ratings to determine the operational effectiveness
	1. Define AS-IS system design				↑				
	2. Do concept design for TO-BE system				↑				
	3. Perform functional analysis on candidate systems	↑	↑	↑	↑	↑	↑	↑	
	4. Build generic simulation model	↑	↑			↑		↑	
	5. Set up volatility tables for human resources		↑					↑	↑
	6. Determine risk response measures		↑					↑	
	7. Evaluate and compare models		↑		↑		↑	↑	↑
	8. Perform activity-based risk analysis		↑	↑	↑		↑		↑
	9. Identify high risk contributing activities		↑	↑			↑	↑	↑
	10. Optimise the system (risk and cost)		↑	↑			↑	↑	↑
	11. Select appropriate system for implementation		↑		↑		↑	↑	

The **research problem** was validated from observations in real-world projects, safety guidelines, risk documentation from mines, and published literature. From these sources, a discontinuity was identified between acquisition and operations phases in terms of the management of risk. These shortfalls were translated into research challenges, each of which was described in Chapter 3. The research problem validation is summarised in the top section of Table 35, where the research challenges are mapped to validating information sources. The research problem was further validated in the literature study in Chapter 4, where similar problems from different engineering fields were identified. This is also represented in Table 35 where arrows from literature focus areas show which sources contributed to validate research challenges.

Research solutions were defined to address research challenges. These solutions were determined and verified from literature in specific focus areas. Observations from literature in the focus areas were discussed in Chapter 4. Table 35 shows the research solutions that were derived from the research challenges, using the information from literature focus areas. Additional validation of the research challenges is shown in Table 35, with the arrows indicating which literature focus areas contributed to validate research solutions.

The **ABR process** was verified to ensure the research problem is addressed by linking all steps of the ABR process to relevant research solutions. That is, the ABR process was derived to address research solutions. The development of the ABR process was presented in Chapter 5, and the verification of this process is shown in Table 35. In the matrix, steps of the ABR process are listed and mapped to relevant research solutions for the sake of simplicity. The table thus verifies the process as it provides traceability, starting from the research problem, proceeding to research challenges and solutions, and finally resulting in a single solution that addresses all research challenges.

The **ABR process** was **validated** by means of a real world case study. In this case study, the ABR process was applied in the acquisition of a winch signalling safety system for scraping operations at the stopes. The initial concept system, as proposed by the mine, was analysed with the ABR process. Two additional candidate systems were identified, namely a risk-reduced system (EES2) and a cost-reduced system (ESS3). All three electronic systems were fully developed and evaluated in a controlled operational environment. Feedback from mining operations showed that the initial system did not address all requirements and was rejected, in line with results from the ABR analysis. Both ESS2 and ESS3 systems were accepted, which is also in line with simulation results. To date, more than 2000 risk-reduced systems and more than 4500 cost-reduced systems have been deployed.

7.5 Future work

The ABR acquisition process was developed and evaluated in this research. Areas of further research are discussed in the following paragraphs.

1. **Human risk profile development:** In this research human risk levels were defined from 1 to 5 and implemented in the simulation model by means of volatility tables. The validity of this approach was found from literature, but this focus falls inside the industrial psychology domain, which is outside the scope of this research. Further work can be done to determine human risk profiles applicable to mining;
2. **ABR software tool development:** A software tool can be developed to assist with the steps of the ABR process. This tool could be integrated into a simulation package (like SIMIO);
3. **Generalization of the ABR process:** Although the ABR process is specifically for the SA mining environment and applicable to electronic safety equipment, it could also be applied to alternative engineering fields. Further research can be performed on the effectiveness of the ABR process in other engineering fields.

7.6 Conclusion

This chapter provided evidence that this research achieved its initial goals of providing an acquisition process for electronic safety equipment in mines. The acquisition process was systematically designed as shown in the traceability matrices. The activity-based risk method and process were thus verified to address all research challenges. Validation of the ABR method and process was provided by means of a case study, which demonstrated the real-world relevance of this research. Activity-based risk can thus be applied in a systems engineering context to perform future development of electronic safety systems in South African mines.

Bibliography

[1] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[2] H. A. Simon, *The sciences of the artificial (3rd Ed.)*, vol. 136. MIT press, 1996.

[3] “Artifact: Merriam-Webster online dictionary; .” [Online]. Available: http://www.merriam-webster.com/dictionary/artifact. [Accessed: 01-Nov-2014].

[4] G. L. Geerts, “A design science research methodology and its application to accounting information systems research,” *International Journal of Accounting Information Systems*, vol. 12, no. 2, pp. 142–151, 2011.

[5] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[6] S. T. March and V. C. Storey, “Design science in the information systems discipline: an introduction to the special issue on design science research,” *MIS Quarterly*, vol. 32, no. 4, pp. 725–730, 2008.

[7] V. Vaishnavi and W. Kuechler, “Design research in information systems,” 2004.

[8] J. Iivari, “A paradigmatic analysis of information systems as a design science,” *Scandinavian Journal of Information Systems*, vol. 19, no. 2, p. 5, 2007.

[9] A. R. Hevner, “A three cycle view of design science research,” *Scandinavian journal of information systems*, vol. 19, no. 2, p. 4, 2007.

[10] S. T. March and G. F. Smith, “Design and natural science research on information technology,” *Decision support systems*, vol. 15, no. 4, pp. 251–266, 1995.

[11] S. Gregor and A. R. Hevner, “Positioning and presenting design science research for maximum impact,” *MIS Quarterly*, vol. 37, no. 2, pp. 337–356, 2013.

[12] “SIMRAC: Hazard Identification and Risk Assessment (HIRA) Processes,” 2002.

[13] “Mine Health and Safety Act and Regulations 29 of 1996 - Tenth Edition,” 2009.

[14] “Safety in Mines Research Advisory Committee (SIMRAC) on the behalf of the Mine Health and Safety Council,” *Notice 1857 of 2005, Staatskoerant*, 2005.

[15] T. Boshoff, “Different Risk Assessment Types.” [Online]. Available: www.labourguide.co.za. [Accessed: 18–10-2014].

[16] A. Paithankar, “Hazard Identification and Risk Analysis in Mining Industry,” *Department of Mining Engineering National Institute of Technololgy Rourkela*, 2011.

[17] “Risk Assessment Process,” *CMT Technologies*, 2008.

[18] S. Rupprecht, “Safety considerations in underground logistics-a look at vertical, horizontal and in-stope transportation systems,” *South African Institute of Mining and Metallurgy. Journal*, vol. 111, no. 1, pp. 45–53, 2011.

[19] J. Oberholzer and L. Thorpe, “An assessment of the most significant causes of transportation and machinery accidents on collieries,” no. COL203, 1995.

[20] S. Mason, P. Ballot, J. Cottrell, J. Currie, and A. Heap, “The influence of ergonomic design of trackless mining machines on the health and safety of the operators, drivers and workers,” no. COL416, 1998.

[21] P. S. Moss, C. F. Talbot, P. J. Foster, and A. M. Rushworth, “Risk analysis and assessment of vertical and incline small winder systems and peripheral activities,” no. GAP636, 2000.

[22] P. D. Krige, B. Leong, and J. Manganye, “Learning outcomes and effective communication techniques for hazard recognition learning programmes in the transportation thrust area.,” no. GAP857, 2001.

[23] P. Schutte and M. Shaba, “Investigation into slipping and falling accidents and materials handling in the South African mining industry,” 2003.

[24] R. Moseme, P. Foster, R. Demana, and S. Rupprecht, “Investigation into the causes of accidents on scraper systems in the gold and platinum mining sectors,” no. GAP030501, 2003.

[25] Y. Potvin, “Strategies and tactics to control seismic risks in mines,” *Journal of the South African Institute of Mining \& Metallurgy*, vol. 109, no. 3, p. 177, 2009.

[26] “ISO 31000: 2009 Risk management-Principles and Guidelines,” *International Organization for Standardization, Geneva, Switzerland*, 2009.

[27] “First report on the harmonisation of risk assessment procedures,” *European Commision*, 2000.

[28] F. M. Christensen, O. Andersen, N. J. Duijm, and P. Harremoës, “Risk terminology—a platform for common understanding and better communication,” *Journal of Hazardous Materials*, vol. 103, no. 3, pp. 181–203, 2003.

[29] E. Avanesov, “Risk management in ISO 9000 series standards,” in *International Conference on Risk Assessment and Management*, 2009, vol. 24, p. 25.

[30] “Risk Management - Vocabulary and guidelines for Use,” *International Organization for Standardization (ISO)*, 2009.

[31] “Safety aspects - Guidelines for their inclusion in standards,” *International Organization for Standardization (ISO)*, 2014.

[32] “A New Approach for Managing Operational Risk: Addressing the Issues Underlying the 2008 Global Financial Crisis,” *OpRisk Advisory, Towers Perrin, Canadian Institute of Actuaries*, 2010.

[33] D. Cooper, “The Australian and New Zealand standard on risk management, AS/NZS 4360: 2004,” 2004.

[34] “Risk Assessment and Management, Leading Practice Sustainable Development Program for the Mining Industry,” *Austrealian Government: Department of Resources Energy and Tourism*, 2008.

[35] F. Backlund and J. Hannu, “Can we make maintenance decisions on risk analysis results?,” *Journal of Quality in Maintenance Engineering*, vol. 8, no. 1, pp. 77–91, 2002.

[36] E. D. Smith, W. T. Siefert, and D. Drain, “Risk matrix input data biases,” *Systems Engineering*, vol. 12, no. 4, pp. 344–360, 2009.

[37] A. Banerjee, “Equivalance of Risk: A mathematical Approach,” 2011.

[38] H. Altabbakh, M. A. AlKazimi, S. Murray, and K. Grantham, “STAMP-Holistic system safety approach or just another risk model?,” *Journal of Loss Prevention in the Process Industries*, vol. 32, pp. 109–119, 2014.

[39] F. I. Khan and S. Abbasi, “Techniques and methodologies for risk analysis in chemical process industries,” *Journal of Loss Prevention in the Process Industries*, vol. 11, no. 4, pp. 261–277, 1998.

[40] “Failure mode and effects analysis.” [Online]. Available: http://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis. [Accessed: 14–08-2014].

[41] K. B. Misra, *The Handbook of Performability Engineering*. Springer, 2008.

[42] “Fault tree analysis.” [Online]. Available: http://en.wikipedia.org/wiki/Fault_tree_analysis. [Accessed: 15–08-2014].

[43] “Event tree analysis.” [Online]. Available: http://en.wikipedia.org/wiki/Event_tree_analysis. [Accessed: 15–08-2014].

[44] P. K. Marhavilas, D. Koulouriotis, and V. Gemeni, “Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009,” *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 5, pp. 477–523, 2011.

[45] J. Tixier, G. Dusserre, O. Salvi, and D. Gaston, “Review of 62 risk analysis methodologies of industrial plants,” *Journal of Loss Prevention in the process industries*, vol. 15, no. 4, pp. 291–303, 2002.

[46] N. Arunraj and J. Maiti, “Risk-based maintenance: Techniques and applications,” *Journal of Hazardous Materials*, vol. 142, no. 3, pp. 653–661, 2007.

[47] O. Renn, “Three decades of risk research: accomplishments and new challenges,” *J. Risk Res.*, vol. 1, no. 1, pp. 49–71, 1998.

[48] A. Stirling, “Risk at a turning point?,” *J. Risk Res.*, vol. 1, no. 2, pp. 97–109, 1998.

[49] T. Aven, “Trends in Quantitative Risk Assessments,” *International Journal of Performability Engineering*, vol. 5, no. 5, p. 447, 2009.

[50] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. Mit Press, 2012.

[51] S. W. A. Dekker, “The re-invention of human error,” *Human factors and aerospace safety*, vol. 1, no. 3, pp. 247–265, 2001.

[52] B. Hallbert and others, *Human event repository and analysis (HERA) system, overview*. Division of Risk Assessment and Special Projects, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission, 2006.

[53] F. Badenhorst and J. Van Tonder, “Determining the factors causing human error deficiencies at a public utility company,” *SA Journal of Human Resource Management*, vol. 2, no. 3, pp. 62–69, 2004.

[54] S. W. A. Dekker, *The field guide to human error*. Bedford, UK: Cranfield University Press, 2006.

[55] S. W. A. Dekker, *Just Culture (Epub) Balancing Safety and Accountability*. Ashgate Publishing, 2012.

[56] A. I. Glendon, S. Clarke, and E. F. McKenna, *Human safety and risk management*. CRC Press, 2006.

[57] K. B. Misra, *The Handbook of Performability Engineering*. Springer, 2008.

[58] J. T. Reason, *Human Error*. Wiley, 1990.

[59] L. Jelemensky, “Contemporary state of the scientific knowledge about human factors and labour safety in Slovakia.”

[60] S. Kristiansen, “Maritime transportation: Safety management and risk analysis,” 2005.

[61] D. I. Gertman, H. S. Blackman, J. Marble, J. Byers, C. Smith, and others, *The SPAR-H human reliability analysis method*. US Nuclear Regulatory Commission, 2005.

[62] M. Demichela, R. Pirani, and M. C. Leva, “Human Factor Analysis Embedded in Risk Assessment of Industrial Machines: Effects on the Safety Integrity Level,” *International Journal of Performability Engineering*, vol. 10, no. 5, p. 487, 2014.

[63] I. A. Herrera and R. Woltjer, “Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis,” *Reliability Engineering \& System Safety*, vol. 95, no. 12, pp. 1269–1275, 2010.

[64] L. Layman, V. R. Basili, and M. V. Zelkowitz, “A Methodology for Exposing Risk in Achieving Emergent System Properties,” *ACM Transactions on Software Engineering and Methodology (TOSEM)*, vol. 23, no. 3, p. 22, 2014.

[65] D. Embrey and S. Zaed, “A set of computer based tools identifying and preventing human error in plant operations.”

[66] N. Dulac, “A framework for dynamic safety and risk management modeling in complex engineering systems,” *Massachusetts Institute of Technology*, 2007.

[67] N. Leveson, “A new accident model for engineering safer systems,” *Safety science*, vol. 42, no. 4, pp. 237–270, 2004.

[68] P. S. Nelson, “A STAMP analysis of the LEX COMAIR 5191 accident,” *Lund University, Sweden*, 2008.

[69] S. Sklet, “Comparison of some selected methods for accident investigation,” *Journal of hazardous materials*, vol. 111, no. 1, pp. 29–37, 2004.

[70] “List of discrete event simulation software.” [Online]. Available: http://en.wikipedia.org/wiki/List_of_discrete_event_simulation_software. [Accessed: 29–04-2015].

[71] C. Pegden and D. Sturrock, “Rapid Modeling Solutions: Introduction to Simulation and Simio,” 2013.

[72] M. Standard, “MIL-STD 499B (draft),” *Systems Engineering*, 1993.

[73] “EIA-632 Processes for Engineering a System,” *Electronic Industries Alliance*, 1999.

[74] "ISO/IEC 15288:2008 Systems and software engineering - System life cycle processes," *The Institute of Electrical and Electronic Engineers*, 2008.

[75] "ISO/IEC 26702 IEEE Std 1220-2005 Systems Engineering - Application and management of the systems engineering process," *The Institute of Electrical and Electronic Engineers*, 2007.

[76] R. Shishko and R. Aster, "NASA systems engineering handbook," *NASA Special Publication*, vol. 6105, 1995.

[77] "INCOSE systems engineering handbook v. 3.2. 2," *INCOSE SE Handbook Working Group and others*, 2011.

[78] S. A. Sheard and J. G. Lake, "Systems engineering standards and models compared," in *Proceedings of the Eighth International Symposium on Systems Engineering, Vancouver, Canada*, 1998, pp. 589–605.

[79] B. S. Blanchard and W. J. Fabrycky, *Systems engineering and analysis*, 4th ed. Prentice Hall Englewood Cliffs, New Jersey, 2006.

[80] "The system lifecycle in systems engineering." [Online]. Available: http://en.wikipedia.org/wiki/System_lifecycle. [Accessed: 27-Nov-2014].

[81] J. N. Martin, "The seven samurai of systems engineering: dealing with the complexity of 7 interrelated systems," in *Proceedings of the 14th International INCOSE Symposium*, 2004.

Appendix A

ESS Product Risk Assessment

The product risk assessment performed on the ESS system is presented in this appendix. This product risk assessment is done in a matrix format and consists of a component and material assessment, risk assessment matrix, considered risk cases, product risk analysis table, risk mitigation, and explanation of hotspots.

A. Component material assessment

Component	**Material type**	**Specifications / benefits**
Enclosures		
1.6mm plate	Mild steel	Exposure excluded by powder coating
Powder coated	Dry powder type – zinc phosphate – 80 microns	Coating protects against corrosion
Press fit fasteners	Mild steel	Easy assembly – no nuts
Star Torx fasteners	Stainless steel	ISO 7380, 10.9
Laser-cut precision		Provides for uniformity – quality assurance
Butt hinge- m/steel bolt & nut	Nylon 6 – 30% injection moulded	Self-extinguishing UL94 HB ; Oxygen index 21-23%

Neoprene lid gasket (IP55)	Neoprene 25 – die cut	UL94 & fmvss302 94 HBF – self extinguishing
10mm Crosby clamps	Clip – galvanised cast steel U-bolt & nut - electroplated	Protected against corrosion
LED bezels		
Injection moulded cup & domed shaped lens	High impact polycarbonate - Makrolon®	Fire classification up to UL 94v-0/1.5 mm & UL 94-5va/3.0 mm; Maximum temperature in glow wire test up to 960 °c
fully encapsulated with resin	Technoresin cr204 & ch204 suitable for encapsulating electrical equipment – small transformers	UL94 HB self-extinguishing
LED PCB	Copper PCB with components ISO 9001	Conformally coated in sealed enclosure
Conductors	300V JSC 5052, 22 AWG, 3 conductors	
Bezel gasket	Monprene MP1073 FL	UL94 V-0 self-extinguishing
Piezo buzzer		
Fire retardant ABS plastic	Fire retardant abs	UL94 V-0 self-extinguishing
Buzzer element	Stainless steel	Will not rust in environment
Rated	105db at 30cm	Tested 96db at 3m
Pull switches		
Brass assembly	CNC machined – exact reproduction	Resistant to corrosion
Spring	Hardened stainless steel	Resistant to corrosion
Eye bolt	Cast steel - dip galvanised	Resistant to corrosion
Micro switch plate	Nylon 6 – 30% injection moulded	Self-extinguishing UL94 HB; Oxygen index 21-23%
Micro-switch	High mechanical life – 1000000 ops min High electrical life – 100 000 ops min Contact resistance – 15mΩ max Current rating : 15A @ 250V	
IP44 sockets 5-pin	IEC 309 standards	Self-extinguishing –glow wire test 850^{0}c

Industrial Gewiss socket	Terminals gold plated as per specification	Resistant to corrosion
IP44 plugs 5-pin	IEC 309 standards	Self-extinguishing –glow wire test 850^{0}c
Industrial Gewiss plug	Terminals gold plated as per specification	Resistant to corrosion
Green pull cable		Manufactured to : NCB 643/1979 class 6
6 core 0.75mm conductors	Stranded tinned copper and PVC insulated	
PVC bedded	Extruded PVC layer	
Braided	Brass plated steel wire braid	
Horse hooks		
Strain relief block	Nylon 6 – 30% injection moulded	Self-extinguishing UL94 HB ; Oxygen index 21-23%
Custom glanding	Mild steel cadmium plated	Resistant to corrosion
Custom hook 8mm	Mild steel galvanised	Resistant to corrosion
Pigtails		
Custom support device	Galvanised spring wire & bush	Resistant to corrosion
Electronic circuit boards	Copper board with electronic components	All manufactured to ISO 9001 standard
	Conformally coated	

B. Risk Assessment matrix

Rating	1	2	3
Critical (A)	Failure will cause hazardous or unsafe condition	Failure will cause important production activity ceasing for a significant period.	Single component over R250,000.
Major (B)	Failure will cause direct production down time, assuming normal engineering back up.	Single component not classified in A1 with value over R100,000 but less than R250,000.	Equipment not classified in A1 but which is to work continually underground and may be difficult to bring up.
Minor (C)	Failure will not affect the safety of personnel.	Failure will not cause production down time.	Components not classified in A1 & A2 with value less than R100,000.

Probability Rating

Rating	1 (<1%)	2 (1% - 5%)	3 (5% - 10%)	4 (10% - 50%)	5 (>50%)
Explanation	Practically impossible	Not likely to happen	Could happen	Has happened	Common

C. **Considered risk cases** (not necessarily probable)

1. Functional failures:
    a. Component failure due to workmanship (infant mortality);
    b. Product end of life failure;
    c. Incorrect use of product;
    d. Stressing of product during use.
2. Explosion & fire:
    a. Presence of explosive gases during operation
    b. Overstressing of materials – high currents or voltages;
    c. Exposure of flammable materials to excessive heat;
    d. Failure modes (failure mode analysis).
3. Personal harm:
    a. Exposure to damaged components(exposed cables/enclosure metal, etc);
    b. Exposure to high voltages and / or currents;
    c. Failure to wear PPE as per standard;
    d. Failure to understand or adhere to operational and maintenance information from system (audible / visual signals);
    e. Failure to follow procedures.
4. Theft or loss:
    a. Perceived valuables such as gold plating on plug and socket;
    b. Cable and plug theft;
    c. Disassembly of units in storage.

5. Use / operational risk
    a. Failure to follow procedures during installation, operation and maintenance;
    b. Incorrect training and / or availability of training material on site;
    c. Failure to understand or adhere to operational and maintenance information from system (audible / visual signals).

D. PRODUCT RISK ANALYSIS TABLE

RISK TABLE										
Component	***Functional failure***		***Explosion / fire***		***Personal harm***		***Theft or loss***		***Use risk (user)***	
	Probability	***Impact***	***Probability***	***Impact***	***Probability***	***Impact***	***Probability***	***Impact***	***Probability***	***Impact***
Control box										
Bezel assembly	2 / 1	C2	1	C1	1	C1	1	**B1**	3 / 1	**A1**
Start button	2 / 1	**B1**	1	C1	1	C1	1	**B1**	1	**B1**
Signal button	2 / 1	C2	1	C1	1	C1	1	**B1**	1	**B1**
Key - I-button	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	3 / 1	**B1**
Key holder / key function	2 / 1	**B1**	1	C1	1	C1	1	**B1**	1	**B1**
LED indicator panel	2 / 1	C2	1	C1	1	C1	1	**B1**	1	C2
Buzzer	3 / 1	C2	1	C1	1	C1	1	**B1**	3 / 1	**A1**
Feed cable to starter	2 / 1	**B1**	1	C1	1	C1	1	**B1**	1	**B1**
Controller - card	2 / 1	**B1**	1	C1	1	C1	1	**B1**	1	**B1**
Cable sockets	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	**B1**
Socket terminals	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	**B1**
Enclosure	2 / 1	C2	1	C1	2 / 1	C1	1	**B1**	1	**B1**

Butt hinge-mild steel bolts	2 / 1	C2	1	C1	1	C1	1	**C1**	1	**B1**
Lid -neoprene 25 seal	2 / 1	C2	1	C1	1	C1	1	**C1**	1	**B1**
Torx fasteners	1	C2	1	C1	1	C1	1	**C1**	1	**B1**
Signal box										
Bezel assembly	2 / 1	C2	1	C1	1	C1	1	C1	3 / 1	**A1**
Buzzers	2 / 1	C2	1	C1	1	C1	1	C1	3 / 1	**A1**
Key holder / key function	2 / 1	**B1**	1	C1	1	C1	1	C1	3 / 1	**B1**
Signal slave card	2 / 1	**B1**	1	C1	1	C1	1	C1	1	C1
Pull switch brass	2 / 1	**B1**	1	C1	1	C1	1	C1	1	C1
Galvanised eye bolt	1	C2	1	C1	1	C1	1	C1	1	C1
Cable sockets	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	C1
Socket terminals	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	C1
Enclosure	2 / 1	C2	1	C1	1	C1	1	C1	1	C1
Lid - neoprene 25 seal	2 / 1	C2	1	C1	1	C1	1	C1	1	C1
Torx fasteners	1	C2	1	C1	1	C1	1	C1	1	C1
Crosby clamps on bracket	1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	**A1**
Pull cable assembly										
Green pull cable - 6 core	2 / 1	**B1**	1	C1	3 / 1	**A1**	3 / 1	**B1**	3 / 1	**A1**
Horse hook strain relief	2 / 1	C2	1	C1	1	C1	41671	C1	1	C1
Pigtails	1	C2	1	C1	1	C1	1	C1	3 / 1	**B1**

Tail ends	1	C2	1	C1	1	C1	1	C1	1	C1
Cable plugs	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	C1
Cable plug terminals	2 / 1	**B1**	1	C1	1	C1	3 / 1	**B1**	1	C1
Interfaces										
Winch to control unit	2 / 1	**B1**	1	C1	1	C1	1	C1	3 / 1	**B1**
System to user	2 / 1	**A1**	1	C1	1	C1	1	C1	3 / 1	**A1**

E. **Risk reduction measures / mitigation**

1. Functional failures:
    - Regular recorded inspections – preventative maintenance;
    - Unscheduled maintenance measures – component swap-out;
    - Feedback on manufacturing / workmanship issues to supplier;
    - Proper training in use of product (Manuals / Training);
    - Clear procedural instruction and verification with certification;
    - Manufacturing and logistics – Quality Assurance;
    - Diagnostics and fault indication with clear procedures and logistic support;
    - Modularity / Interchange-ability of components.
2. Explosion & fire:
    - Correct selection of materials during design;
    - Control over production quality;

- Fail-safe design (over-voltage and short-circuit protection);
- Proper explosive gas detection and ventilation.

3. Personal harm:
    - Proper training in use of product (Manuals / Training);
    - Proper use of PPE;
    - Visual inspection of equipment status;
    - Fail-safe mode on failures.
4. Theft or loss:
    - Theft prevention procedures;
    - Allocation of enforceable accountability.
5. Use / operational risk:
    - Proper training in installation of product;
    - Proper training in operational use of product;
    - Clear procedural instruction and verification with certification;
    - Installation acceptance certification – authorised installations;
    - Clear maintenance and repair procedures;
    - Logging of all major system events for audit purposes.

F. Explanation of hotspots

1. Bezel Assembly & Buzzer

   These were both given **A1 + 3/1** ratings in the User Risk category. This risk exists as long as the user has less than adequate understanding and knowledge of this new signal method. Training and on the job supervision will mitigate this risk. Re-training as per normal training schedules is critical to the successful use of this product.

2. Crosby Clamps – Signal Boxes

   This item was rated **A1** under User Risk and **B1** under theft and loss. These items are critical to the successful installation and operation of the system as they ensure that the signal boxes are installed / mounted out of the scraper path, preventing physical damage to the signal boxes. Correct installation will also ensure correct sighting of visual signals.

3. Green Pull Cable

   This item was rated **A1 + 3/1** in both the Personal Harm and User Risk categories. Blast damage to cable may expose sharp wire braids that could cause harm to personnel not wearing correct PPE. User not trained to use pull cable may provide circumstance that would bring harm to himself and others in the work area. Theft or loss of this item would result in B1 impact - no cable - no signal. Cables of any kind are usually targeted by thieves.

4. Key I-Button & Key Holder

   These items only received a **B1 + 3/1** rating in both User Risk & Theft and Loss categories. Adequate management controls and training must be enforced to ensure that the user knows how to operate the system with these items, and is held personally responsible for their use and maintenance in good order.

Appendix B

The following documents and SIMIO models can be found on the accompanying compact disc:

B-1: Winch Signalling Model Contents Report V4.pdf

B-2: Winch Signalling System Case Study - Information on Experiments.pdf

B-3: Generic SIMIO model V4 – Winch Signalling System

B-4: Generic SIMIO model V4 – Winch Signalling System (Experiment 1 – AWS and ESS)

B-5: Generic SIMIO model V4 – Winch Signalling System (Experiment 17 – ESS2)

B-6: Generic SIMIO model V4 – Winch Signalling System (Experiment 18 – ESS3)