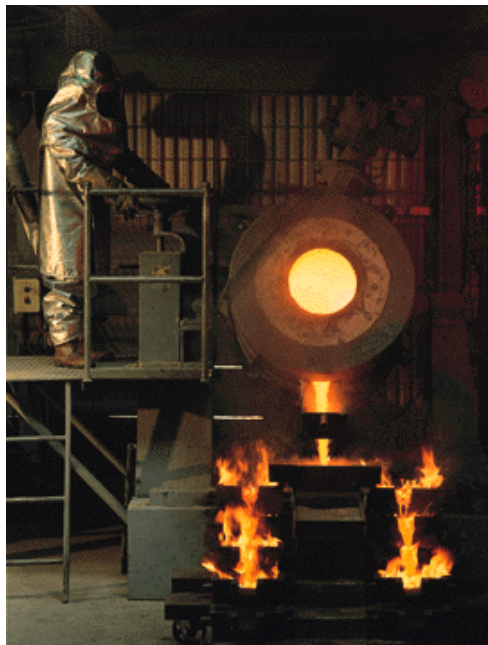


NATIONAL MINERALS INDUSTRY SAFETY AND HEALTH RISK ASSESSMENT GUIDELINE



**By Professor Jim Joy
and
Dr Derek Griffiths**

National Minerals Industry Safety and Health Risk Assessment Guideline

Version 6 - Jan 2007

Contents

Endorsement of Stakeholders

Letter from MCA Chairperson

Overriding Assumptions of This Guideline

1. Introduction / Background

- 1.1 History of risk assessment in the minerals industry
- 1.2 Rationale for the new guideline
- 1.3 Guideline objectives
- 1.4 Relationship to Australian Standards and other resources

2. How to Use This Guideline

- 2.1 Structure of the guideline
- 2.2 Suggested guideline users
- 2.3 Suggested methods of use
- 2.4 Example approaches to using this guideline

3. Setting the Context

- 3.1 Introduction
- 3.2 Setting the strategic, organisational and risk management context
- 3.3 Defining required resources
- 3.4 Defining risk assessment project timing
- 3.5 Establishing clear accountability
- 3.6 Risk Assessment Pitfalls

4. Scoping / Designing the Risk Assessment

- 4.1 Documentation of the scope
 - 4.1.1 Defining the objective based on the expected deliverables
 - A. Formal safety assessment development
 - B. Risk or Hazard Register development
 - C. Risk acceptability determination
 - D. Identification of critical control measures and development of performance indicators
 - E. Information for major or principal hazard plans
 - F. Assessment of Safety Instrumented Systems
 - G. Information for operational guidelines
 - H. Information for maintenance plans or guidelines
 - I. Hardware design review
 - J. Option review

- K. Review of change management plan
- L. Information for drafting of Standard Operating Procedures (SOPs)
- M. Risk awareness in informal day-to-day tasks

- 4.1.2 Identifying and describing the system to be reviewed
- 4.1.3 Identifying and understanding the potential hazards
- 4.1.4 Selecting the risk assessment method – the means of identifying the risks
- 4.1.5 Selecting the risk analysis method – the means of calculating and examining the level of risk
 - 4.1.5.1. Risk analysis methods
 - a. Qualitative risk analysis
 - b. Quantitative risk analysis
 - c. Semi Quantitative risk analysis
 - 4.1.5.2. Risk acceptability
 - 4.1.5.3. Selecting the method considering the expected deliverable
 - 4.1.5.4. Re-analysis of risk considering new controls
 - 4.1.5.5. Risk/cost benefit analysis
- 4.1.6 Selecting a facilitator for the risk assessment
- 4.1.7 Determining the composition of the team or work group
- 4.1.8 Deciding the time required (and venue)
- 4.1.9 Risk assessment results and feedback

5. Facilitating / Leading a Risk Assessment Team

- 5.1 Introducing the scope to the team
- 5.2 Reviewing the selected system
- 5.3 Identifying the hazards
- 5.4 Identifying the risks
- 5.5 Analysing the risks
- 5.6 Evaluating the risk acceptability
- 5.7 Considering existing controls or barriers
- 5.8 Identifying new controls or barriers
- 5.9 Closing the risk assessment
- 5.10 Summary of Risk Management Process for Common Situations
- 5.11 Generic 6 Stage Hazard Studies

6. Applying the Risk Assessment Deliverables

- 6.1 Documenting the risk assessment process and deliverables
- 6.2 Deriving the action plan
- 6.3 Following up on the action plan and deliverables
- 6.4 Using other information from the risk assessment
- 6.5 Change management
- 6.6 Auditing the process

7. Other

7.1 Checklists

- 7.1.1 Scope
- 7.1.2 Consultant proposal
- 7.1.3 Report format
- 7.1.4 Review Checklist
- 7.1.5 Risk assessment exercise logistics

Appendices

Appendix A Definitions

Appendix B Templates

- Hazard and Operability (HAZOP)
- Failure Modes and Effect Analysis (FMEA)
- Failure Modes and Criticality Analysis (FMECA)
- Human Error Analysis (HEA)
- What If...? Analysis
- Workplace Risk Assessment and Control (WRAC)
- Preliminary Hazard Analysis (PHA)
- Level of Protection Analysis (LOPA)
- Hazard / Risk Register

Appendix C Informal Risk Awareness Tool

- Buddy System
- Stop! Take 5

Appendix D Acquisition Checklist

Appendix E HAZOP Audit Checklist

Appendix F Health Risk Assessment Outline

Appendix G Risk Assessment Tools

- Hazard and Operability (HAZOP)
- CHAZOP (Computer Hazard and Operability Studies)
- FMEA (Failure Mode and Effect Analysis)
- Risk Assessment PHA “Preliminary Hazard Assessment” or “Preliminary Hazard Analysis”
- JSA or Job Safety Analysis
- CHAIR Construction Hazard Assessment and Implication Review
- Energy Barrier Analysis (also called Energy Trace Barrier Analysis)
- Consequence Analysis (also called Cause-Consequence Analysis)
- Human Error Analysis

Appendix H. Fatigue Risk Assessment Process

Endorsement of Stakeholders

The organisations and companies whose logos appear below have endorsed this Guideline as a valuable tool for improving the quality of risk assessment within the Australian minerals industry.

In endorsing the Guideline, stakeholders recognise it is neither a definitive nor mandatory document offering minimum requirements, but is intended to provide advice and share experience on risk assessment to help improve the safety performance of the industry.

Letter from Chief Executive of the Minerals Council of Australia (MCA)

The Minerals Council of Australia as the initiator of this project is seeking to take risk assessment in the Australian minerals industry to the next level.

In commissioning the Minerals Industry Safety and Health Centre (MISHC) at the University of Queensland under the leadership of Professor Jim Joy to develop the Guideline, the Council was responding to strong industry support for improvement in the quality of the risk assessment process.

This on-line resource is structured to help individuals design and undertake formal and informal risk assessments. The processes outlined in the Guideline are outcome-based rather than prescriptive with extensive links to case studies and lessons learned.

The Council sees the Guideline as a dynamic document to be enhanced and refined, particularly with the addition of new case studies and the sharing of experiences in the application of risk assessment processes.

The Council believes this Guideline will make an important contribution in ensuring the Australian minerals industry continues to provide leadership in improving the safety performance of the minerals sector.

MITCHELL H HOOKE
CHIEF EXECUTIVE

Overriding Assumptions Concerning This Guideline

The minerals industry, like other major global industries, must consider and manage risks to business objectives (i.e. OH&S, environment, community and other areas) to remain successful.

Management of risks requires a proactive, systematic approach, applied when key decisions are being made across the life cycle of the industry from exploration through to mine closure.

Risk assessment methodology offers systematic approaches that can assist with key decision making that are made in the minerals industry.

Although regulatory authorities promote and, in some cases, require risk assessment, these methods are an inherent part of sound business management and not only a morale or legal obligation.

The accuracy and effectiveness of risk assessment deliverables can vary greatly depending on the quality of the risk assessment process.

This MCA guideline can provide guidance for those intent on following a quality process of risk assessment in their operations.

This guideline is intended to provide advice on risk assessment and is not a definitive or mandatory document.

In the body of the guidelines, there are a number of Internet links and reference sources of further information on the guideline topics. It must be noted that the authors and/or contents of these links and references are in no way endorsed by the Minerals Council of Australia (MCA) or Minerals Industry Safety and Health Centre (MISHC). They are only supplied to provide additional information on the topics.

1. Introduction and Background

In 2001 the Minerals Council of Australia (MCA) initiated a national project to derive helpful “good practice” guideline for risk assessment in the minerals industry.

The Minerals Industry Safety and Health Centre (MISHC) at the University of Queensland was commissioned to draft the guideline working closely with a representative cross section of the industry. Those representative organisations are listed below.

Anglo Coal
BHP Billiton
Newcrest
Newmont Australia
Rio Tinto
Roche Mining
WMC

NSW Minerals Council
QLD Minerals Council (QMC)
Chamber of Minerals and Energy WA

NSW Department of Minerals Resources
QLD Department of Natural Resources and Mines
WA Department of Minerals and Petroleum Resources

NSW Mine Safety Council
QLD Mining Safety and Health Advisory Council
WA Mining Occupational Safety and Health Advisory Board (MOSHAB)

The derivation of this guideline was greatly assisted by the results of a survey completed by the above organisations. The survey examined a proposed guideline framework and content, seeking consensus and comment from the respondents. The response rate to the survey was 100%, probably indicating the degree of interest in the topic.

1.1 History of risk assessment in the minerals industry

Formal risk assessment has a longer history in industries other than mining. For example, the petrochemical, nuclear, military, aviation and space industries have applied various formal risk assessment techniques for over 30 years.

This proactive approach to improving risks, as opposed to a reactive “fix-it-when-it-breaks” mentality, was in most cases triggered by a major public disaster such as the Flixborough chemical plant disaster (1973), Three Mile Island nuclear plant event (1979) and, others.

Today all of the previously listed industries would see risk assessment as an inherent part of their business.

Though not as lengthy, risk assessment has had a significant history in the Australian minerals industry. The Australian industry has applied formal, systematic risk assessment more extensively than minerals industries in other countries. With a history of over 10 years in many parts of the industry, there has been rapid growth in the use of the methodology. However, the growth of methods and competency has been erratic in many ways leading to issues with the quality of risk assessment application.

1.2 Rationale for the new guideline

The minerals industry is committed to improving the quality and consistency of risk assessment conducted across the industry. There is also a need to introduce more sophisticated methods and their associated benefits to the industry, therefore providing the opportunity to achieve a “step-change” in the effectiveness of risk assessments.

This guideline provides information to help standardise the methodology, recognised and supported by industry representative organisations.

1.3 Guideline objectives

This guideline intends to address the following objectives to:

- Help various users achieve effective and efficient deliverables from risk assessment,
- Outline various risk assessment approaches to achieve deliverables ranging from informal risk assessment and SOPs, through to Formal Safety Assessments and Catastrophic Risk Management Plans,
- Provide a robust, process based methodology to risk assessment that will assist in making a step change in risk assessment,
- Suggest that risk assessment scoping or design is critical to achieving quality deliverables,
- Assist in checking the potential (scopes or proposals) and actual quality (reports) of risk assessment projects,
- Help establish risk assessment as part of “the way we do business”.

1.4 Relationship to Australian Standards and other resources

This guideline is not intended to replace existing Australian Standards, regulatory information (such as NSW MDG 1010¹/1014²) or other guidance but to supplement with more complete and process oriented information.

¹MDG 1010 Risk Management Handbook for the Mining Industry NSW Department of Mineral Resources

² MDG1014Guide to reviewing a Risk Assessment of Mine Equipment and Operations NSW Department of Mineral Resources

The content of this guideline is consistent with the intent of AS 4360³ and is generally based on the Risk Management model in AS 4360 (below).

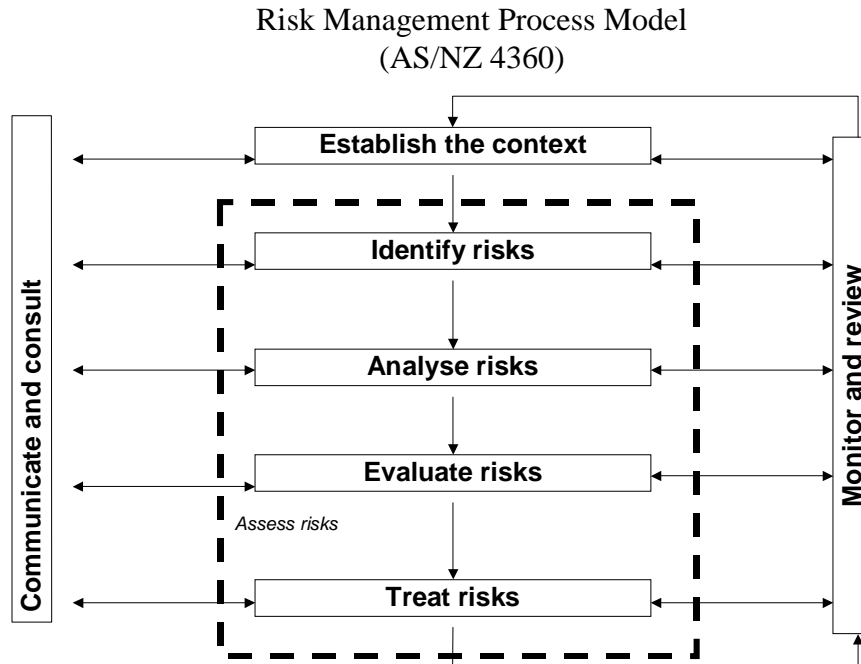


Figure 1.1 Risk management process model

AS 4360 defines Risk Assessment as “the overall process of risk analysis and risk evaluation”. For the purposes of this Guideline, the term Risk Assessment will refer to all the steps inside the dotted line.

In AS 4360, “Establishing the Context” includes 5 key areas:

- The strategic context,
- The organisational context,
- The risk management context,
- Develop risk evaluation (and acceptance) criteria, and
- Decide the structure.


These areas, and specifically the last three, are extensively addressed in this Guideline as the Scoping or Design Phase of the Risk Assessment. Based on the aforementioned survey, the industry believes that this is a critical part of this guideline.

³ AS/NZS 4360 (2004) Risk Management

2. How to Use This Guideline

2.1 Structure of the guideline

The guideline content follows the process of Risk Assessment, from setting the context of the effort through several deliverable-based streams in a step-by-step manner.

 The statement, “**THIS IS A KEY ISSUE**”, will occur occasionally in this guideline. It is intended to indicate something of particular importance, usually due to inadequacies in current risk assessment practices.

LESSONS LEARNED

There are short items called “Lessons Learned” throughout the guideline. They provide examples or illustrations of problems that can arise throughout the risk assessment process. They are mostly examples of past issues in the minerals industry, sometimes contributing to unwanted events.

2.2 Suggested guideline users

The suggested users would include:

- Site personnel involved in determining requirements for risk assessment, or facilitating/leading a risk assessment
- Industry personnel such as consultants and contractors servicing the industry through engagement in the risk assessment process.

2.3 Suggested methods of use

Apply this guideline to achieve the desired deliverables of a risk assessment.

- Use the information in this guideline to assist in defining a site or corporate procedure/process for risk assessments
- Follow the steps in Chapter 4 and 5 to design and/or lead a risk assessment
- Use this guideline as a “cookbook” to help develop competency through guided practice
- Use this guideline as a checking tool for scopes, proposals and risk assessment reports

Example approaches to using this guideline:

- ***Designing a risk assessment***

The reader can find extensive help in this guideline to design or scope a risk assessment. If the reader goes directly to the Chapter on Scoping, he/she can follow that the content thorough and draft a scope, establishing the desired deliverable and objective, selecting the risk assessment and analysis techniques, team, venue, etc. A checklist is also included in the Appendices to review a scope.

- ***Following a risk assessment process during an exercise***

Chapter 5 covers the facilitation process in this guideline. The reader can use that section to plan the exercise agenda, as well as the logistics such as equipment, etc. A checklist for this topic is also included in the Appendices.

- ***Finding a key point***

Many specific risk assessment issues have been addressed in this guideline. Those seeking points of clarification should use the topics listed in the Table of Contents to search a hardcopy of this guideline and key word search for an electronic version.

3. Setting the Context

3.1 Introduction

As part of the overall management of hazards associated with any operation, it would be anticipated that the organisation would have a Safety Management System (SMS). This system would be an integral part of the operation's total management process.

The purpose of the SMS is to ensure safe operation of a facility, by providing a comprehensive and integrated process for systematically managing all aspects of the adopted control measures. To achieve this purpose, the SMS must not only be comprehensive and integrated with respect to the control measures, it needs to be suitable and appropriate to the specific facility, it must be used in practice, and must be reviewed and revised whenever the circumstances require.

A SMS will typically have a set of generic elements forming a continuous improvement cycle. Such a cycle could be

- Policy and objectives
- Standards and targets
- Planning and prioritising
- Implementation
- Monitoring
- Audit
- Corrective action
- Review

with a continual improvement loop back.

As a specific example, the API Model EHS Management System is comprised of 5 components in a continual improvement loop. The components are defined as:

1. Corporate vision, Policy and Management Commitment
2. Plan
 - Management Leadership
 - Responsibilities/Accountabilities
 - Risk Assessment/Management
 - Compliance and other requirements
 - EHS Planning and Programmes
3. Do
 - Personnel Training and Contractor Services
 - Documentation and communications
 - Facilities design and construction
 - Operations, Maintenance and Management of Change
 - Community Awareness and Emergency Response
4. Assess
 - EHS Performance Monitoring and Measurement

Incident Investigation, Reporting and Analysis EHS Management Systems Audits

5. Adjust

Management Review and Adjustment

As can be seen Risk Assessment/Management is a key component of the Planning stage on which the remainder of the cycle depends. This guideline is focussed on this Risk Assessment component within the overall context of the SMS.

For example, to explore more information on various Safety Management Systems approaches try:


- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN12.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN12.pdf)
- NSW Department of Urban Affairs and Planning, 1995. Guidelines for Preparation of Safety Management Systems, Hazardous Industries Planning Advisory Paper No 9. ISBN 0 7310 3062 6. This useful resource is only available as a hardcopy. It can be purchased online (<http://www.planning.nsw.gov.au/>) or alternatively contact the Department.
- American Petroleum Institute, 1998. *Model Environmental, Health and Safety (EHS) Management System*, API 9100A. This useful resource is only available as a hardcopy. The publication can be purchased online (http://global.ihs.com/search_res.cfm?currency_code=USD&customer_id=21254D4D5B0A&shopping_cart_id=2724482F2F4A40304F5B4020250A&rid=API&country_code=US&lang_code=ENGL&input_doc_number=API%209100A&org_code=API).
- American Petroleum Institute, 1998. *Guidance Document for Model EHS System*, API 9100B. This useful resource is only available as a hardcopy. The publication can be purchased online (http://global.ihs.com/search_res.cfm?currency_code=USD&customer_id=21254D4D5E0A&shopping_cart_id=2724482F2F4A40304F5B4020250A&rid=API&country_code=US&lang_code=ENGL&input_doc_number=API%209100B&org_code=API).

3.2 Setting the strategic, organisational and risk management context


Expected outcomes of this step include:

- **Corporate / site commitment**
There should be a documented organisation or site commitment to the process of proactively considering hazards and risks during the making of key decisions in the project or operation. This type of commitment may be mentioned in Risk Management related documents but should be expanded in more detail, for example in a procedure, in order to deal with issues noted below.
- **Application and defined expected deliverables of risk assessment & risk management**

The context for risk assessment (i.e. the procedure) in an organisation or site should identify the situations where application of risk assessment is required.


 **THIS IS A KEY ISSUE.** The selected applications would likely consider the most

important decisions in the organisation. This might include identification of expected deliverables such as procedures, plans, operating guidelines, design finalisation information or others. Defining the deliverables of the risk assessment is necessary before the selection of the most appropriate analytical method (See Chapter 4 of this guideline on **Scoping or Designing the Risk Assessment**).

Some organisations have “procedures” that cover the method(s) of risk assessment but give little guidance on the reasons for applying the methods.  **THIS IS A KEY ISSUE** This may lead to the situation where risk assessment is done without a clear image of the desired deliverable. In other words the objective is to do a risk assessment, rather than produce a useful deliverable such as a key plan, operational recommendations, design review recommendations, safe job procedure, etc. This problem may lead to ineffective use and appreciation of risk assessment.

3.3 Defining required resources

Resources are required for a risk assessment and, as such, should be recognised in the relevant policy or procedure. Resources for some risk assessment methods include a facilitator, a suitable team, a suitable room, information recording equipment, the required time, etc. However, in addition there may be resources to scope or design the risk assessment and resources to gather information on the existence, nature or magnitude of hazards, as well as resources to take the required action as a result of the assessment.

 Sometimes risk assessment teams are created with conveniently available personnel such as those on light duties, even though they may be, at best, only basically familiar with the system being reviewed when compared to other site personnel. This is undesirable and compromising to the entire process. **THIS IS A KEY ISSUE.**

3.4 Defining risk assessment project timing

The timing of a risk assessment depends of the required deliverable but the general principle is the earlier the better. Sometimes the use of a life cycle approach can be helpful to consider the timing of risk assessment.

The Life Cycle Stages of a Project

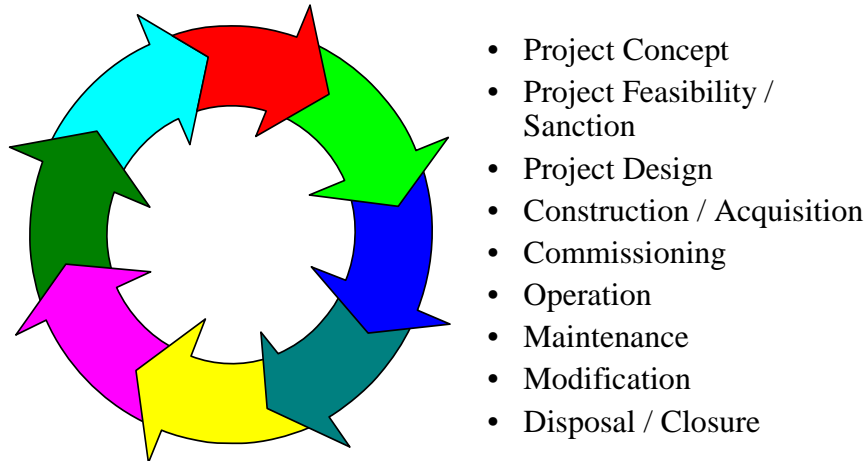


Figure 3.1 The life cycle stages of a project



The Life Cycle illustrates the various stages in any project. The most cost effective timing for risk assessment is in the concept / design phase. **THIS IS A KEY ISSUE.** Risk Assessments should, at least, be done at the earliest possible point in each life cycle stage.

Minimally, the timing of risk assessment should allow time for a quality analysis, as well as time to effectively apply the deliverables from the analysis.

The context of risk assessment (such as a procedure) should include guidance on timing and resource expectations.

The next tables provide an indication of what is being looked for at each of the stages in the project life cycle and indicate which techniques discussed later in this guideline might be appropriate for the particular stage. The choice of a specific technique depends on the specific project, study, timing etc.

Table 3.1 Stage Issues

Stage	Stage Issues
Project Concept	<ul style="list-style-type: none"> ▪ Require understanding of the project its processes and materials sufficient to address safety, health and environment issues during design stage ▪ Consider possibilities of eliminating hazards by redesign or alternative technologies ▪ Completion of PHA (Preliminary Hazard Analysis) type assessment ▪ Generate Hazard Inventory ▪ Incorporate the preliminary thinking regarding closure of the operation and the hazards to be managed at that time ▪ Document decision process and outcomes in all phases of the project

Stage	Stage Issues
Project Feasibility	<ul style="list-style-type: none"> ▪ Include assessment of cost of possible controls for major risk areas ▪ Revise PHA to incorporate current understanding
Project Design	<ul style="list-style-type: none"> ▪ Systematically review the design to identify any hazards (including Health issues) ▪ Identify and estimate the consequences of such hazards and identify controls ▪ Consider all transient conditions eg start up, shut down, emergencies and upsets ▪ Consider ergonomics and manual handling ▪ Manage all changes to the design to ensure that new hazards are not introduced or risks increased ▪ Update PHA to a full assessment using appropriate techniques e.g. HAZOP, ETA,FTA, FMEA etc ▪ Generate initial Hazard Register
Construction	<ul style="list-style-type: none"> ▪ Review the construction methodology and identify, evaluate and propose methods to control specific hazards ▪ Identify construction/existing operation conflicts and management strategy ▪ Ensure measures are in place to ensure design intent and hazard controls are all complied with ▪ Ensure a process is in place for managing any and all changes
Acquisition	<ul style="list-style-type: none"> ▪ Require a review to identify that there has been a full risk management process in place at the acquisition and to determine any gaps that will need to be assessed.
Commissioning	<ul style="list-style-type: none"> ▪ Conduct a risk assessment of the proposed commissioning sequence ▪ Identify transient hazards created by stepped commissioning ▪ Review previous assessments to ensure all actions and controls are implemented
Operation	<ul style="list-style-type: none"> ▪ Ensure that facility is constructed to design intent ▪ Review operations to ensure that these are consistent with design intent and verify that the assumptions made in all earlier studies are valid ▪ Ensure that the SOPs, maintenance procedures and emergency response incorporate all requirements identified in earlier studies. ▪ Ensure changes developed during commissioning and on going operation are consistent with the previous studies and do not introduce or exacerbate risks ▪ Review operations for previously unidentified risks ▪ Systematically review procedures for the facility
Maintenance	<ul style="list-style-type: none"> ▪ Ensure all controls and specifically critical controls are identified and subject to a maintenance regime that meets the control intent, including the maintenance plan, SOPs, etc. ▪ Ensure that the SOPs, maintenance procedures and emergency response incorporate all requirements identified in earlier studies. ▪ As with operations
Modification	<ul style="list-style-type: none"> ▪ There is an absolute requirement to assess all changes to the facility whether managerial, operational, maintenance, shut down, new process, new chemicals etc to ensure that there are no new hazards introduced without controls ▪ Develop documentation of the decisions reached for each change
Disposal Closure	<ul style="list-style-type: none"> ▪ Assess the hazards related to the removal of equipment, closure of pits and dumps, demolition of structures, rehabilitation of dumps, access by others once facility is closed, community issues etc.

See also section 5.10 Risk Management Process for Common Situations and 5.11 Generic 6 Stage Hazard Study

Table 3.2 Application of Assessment Methods

Life Cycle Stage "Timing"	Informal RA	FMEA	JSA/JHA	PHA /HAZAN RAC	FTA	ETA	FMECA	HEA	LOPA	HAZOP/ CHAZOP	Risk Rank	Checklist	CHAIR	SIS
Project Concept "Gleam in the eye"				X							X	X		
Project Feasibility "Board agree to investigate"	X			X							X	X		
Project Design "Funding provided to develop design"		X		X	X	X	X	X	X	X		X	X	X
Construction "Completed during Design"			X					X			X	X	X	
Acquisition "As soon as access is negotiated"				X							X	X		
Commissioning "During design and Construction"			X					X		X	X	X	X	X
Operation "During Design Construction and Commissioning"		X	X	X	X	X		X		X	X	X		X
Maintenance "During design, construction and commissioning"		X	X	X		X	X	X	X	X	X	X		X
Modification "At all times"	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Disposal Closure "From the start up of the facility"	X		X	X							X	X	X	

Note: In the preceding table Checklists are identified as an assessment technique. A checklist identifies known hazards, potential design deficiencies and potential incident situations associated with common equipment or operations. It can be used for processes, equipment, materials and procedures. It is most commonly used when there is a significant, large body of experience or knowledge on the subject under study. However general checklists can sometimes be used for new or unusual designs.

The method is usually limited to ensuring that a process, piece of equipment, material or procedure conforms to accepted standards.

Checklists are noted for being exclusive rather than inclusive in the sense that if an issue is missing from the checklist it probably will be ignored.

An example of a checklist for Acquisitions is given in the appendices. Checklists are not discussed any further in the Guideline.

LESSONS LEARNED 3.1

In the past, a mine applied risk assessment to derive the operating guidelines for a new piece of underground equipment before it was transported into the mine. The assessment identified some design modifications and a large amount of operating requirements. However, the risk assessment was scheduled only a few days before the machine was to go underground and commence production. As a result, the assessment was rushed and there was some resistance to significant new controls.

3.5 Establishing clear accountability

The context (or procedure) should include the accountability for areas such as;

- initiation of a risk assessment in defined circumstances,
- planning or scoping the risk assessment,
- meeting the resource requirements,
- utilisation of facilitators (including consideration of external resources for complex assessments),
- methods for implementing deliverables, and
- checking the quality of risk assessment activities.

LESSONS LEARNED 3.2

Some organisations have “procedures’ with no clear accountability. The “not-my-job” phenomenon occurs, not always deliberately, but often due to human nature. “I do what my boss tells me to do”.

Finally, there are many textbooks available covering risk assessment, including a downloadable System Safety text that covers many of the principles and tools mentioned in this guideline. For example:

- <http://www.dfrn.nasa.gov/Business/DMS/PDF/DHB-S-001.pdf>

3.6 Risk Assessment Pitfalls

Although risk assessment is a potentially powerful tool, as with all tools, if it is not used with care and understanding, the outcomes may well be totally incorrect and lead to bad decisions being made that are not supportable in reality.

It is noted that because of such a lack of understanding of the process and the perception by many that the matrix given in Appendix A of AS/NZS 4360 1999 was the Risk Assessment, the Appendix A will be removed in the next edition.

A recent report by HSE in the UK examined a range of assessments and identified the following “common” pitfalls.


- Carrying out a risk assessment to attempt to justify a decision that has already been made.
- Using generic assessment when a site specific assessment is needed.
- Carrying out a detailed, quantitative risk assessment without first considering whether any relevant good practice was applicable, or when relevant good practice exists.
- Carrying out a risk assessment using inappropriate good practice.
- Making decisions on the basis of individual risk estimates when societal risk is the appropriate measure.
- Only considering the risk from one activity.
- Dividing the time spent on the hazardous activity between several individuals – the “salami slicing” approach to risk estimation.
- Not involving a team of people in the assessment or not including employees with practical knowledge of the process/activity being assessed.
- Ineffective use of consultants.
- Failure to identify all hazards associated with a particular activity.
- Failure to consider all possible outcomes.
- Inappropriate use of data.
- Inappropriate definition of a representative sample of events.
- Inappropriate use of risk criteria.
- No consideration of ALARP arguments (i.e. using cost benefit analysis to attempt to argue that it is acceptable to reduce existing safety standards).
- Not doing anything with the results of the assessment.
- Not linking hazards with risk controls

The full report is available on the HSE website at:

- <http://www.hse.gov.uk/research/rrpdf/rr151.pdf>

4. Scoping / Designing the Risk Assessment

4.1 Documentation of the scope

 The success or otherwise of a risk assessment exercise is mainly determined by the integrity of its fundamental design, sometimes called the “**Scope**”. **THIS IS A KEY ISSUE**. The following notes provide summary detail on the basic requirements for scoping risk assessment exercises.


Scoping a significant risk assessment exercise requires consideration and definition of the following nine main areas. Complex planned risk assessments should carefully consider at least these 12 areas.

- 4.1.1 Defining the objective based on the expected deliverable
- 4.1.2 Identifying and describing the system to be reviewed, the physical and /or process boundaries
- 4.1.3 Identifying and understanding the potential hazards (including health hazards)
- 4.1.4 Selecting Risk Assessment Method-the Means of Systematically Identifying the Risks
- 4.1.5 Selecting Risk Analysis Method-the Means of Calculating and Examining the Level of Risk
- 4.1.6 Range of External Influences to be Considered
- 4.1.7 Consequences of Interest
- 4.1.8 Core Assumptions
- 4.1.9 Selecting a facilitator for the risk assessment
- 4.1.10 Determining the composition of the team or work group
- 4.1.11 Deciding the time required (and venue)
- 4.1.12 Providing risk assessment results and the desired deliverables with accountabilities and timelines

4.1.1 Defining the objective based on the expected deliverable

The objective of a risk assessment exercise might be expressed like this example.

‘The objective of the risk assessment is to review the risks related to (system), specifically focussing on the hazards(such as one or more energy) or types of problems associated with (such as a type of hazard)., in order to produce.....(an output such as information for a Plan)’

 The objective of the risk assessment may be associated with one of the following intended deliverables (note that this is not an all inclusive list). It is important to establish the desired deliverable from the risk assessment before deciding on the risk assessment method. **THIS IS A KEY ISSUE**.

- A. Formal Safety Assessment development
- B. Risk or Hazard Register development
- C. Risk acceptability determination
- D. Identification of critical control measures and development of performance indicators
- E. Information for major or principal hazard plans
- F. Assessment of Safety Instrumented Systems
- G. Information for operational guidelines
- H. Information for maintenance plans or guidelines
- I. Hardware design review
- J. Option selection / review
- K. Review of change management plan
- L. Information for drafting of SOPs
- M. Informal risk awareness on day-to-day tasks

Following are brief outlines explaining these example potential deliverables. After each outline is a selected set of links that provide further selected information in the area. The outline also includes a list of possible, though not exclusive, risk assessment methods for each deliverable. Section 4.1.4 includes a table of deliverables and risk identification methods, plus links to good sources of information on each risk identification technique.

For example, to explore more information on various Risk Assessment approaches try:

- http://www.mishc.uq.edu.au/publications/Risk_Analysis_Methods_a_Brief_Review.pdf
- NSW Department of Urban Affairs and Planning, 1992. *Guidelines for Hazard Analysis*, Hazardous Industries Planning Advisory Paper No 6. ISBN 0 7305 71254. This useful resource is only available as a hardcopy. The publication can be purchased online (<http://www.planning.nsw.gov.au/>) or alternatively contact the Department to order the publication.

4.1.1.A. Formal safety assessment development

With both large and small complex facilities, the process of managing safety issues effectively requires formal methods for both assessing and managing safety.

The term Safety Case is used to describe the argument or case that the operation of a specific facility is managed within acceptable, clearly defined risks. The Safety Case is intended to provide a level of assurance to the senior management/board of a facility/operation or a regulator that the facility is capable of being run safely and has the necessary processes, systems and people in place to ensure that this happens.

A Safety Case is the document that sets out the measures adopted to prevent major incidents and how to reduce the effects should one occur. It is therefore a combination of robust risk assessment methodologies appropriate to the hazards present and a rigorous, comprehensive, detailed and integrated safety management system.

The Safety Case is usually designed to demonstrate to a regulator that measures are appropriate and adequate to ensure that risks from potential major accidents have been reduced to a level 'as low as reasonably practicable' (ALARP⁴) or some defined level of residual risk.

Typically a Safety Case contains information on how the facility will be run safely, including such items as:

- Hazard Identification
- Safety assessment
- Control measure identification, selection and performance standards
- Safety management system that supports the control measures
- Emergency plan
- Management of Change
- Process for reviewing and keeping the safety case up to date

From the above it is clear that a Safety Case is not a particular risk assessment method but rather a management methodology based on a rigorous Formal Safety Assessment (FSA) method. The FSA method usually involves a systematic review of the operation, initially using preliminary or broad brush risk assessment methods as well as more detailed techniques to examine major issues in more depth.

The FSA methodology can be applied at minerals industry sites for comprehensive operational review.

For example, to explore more information on various Safety Cases and Formal Safety Assessment approaches try:

- http://www.mishc.uq.edu.au/publications/Development_of_a_Safety_Case.pdf
- http://www.industry.gov.au/library/content_library/facility.pdf
- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN3.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN3.pdf)
- <http://www.hse.gov.uk/railway/criteria/>
- <http://www.hse.gov.uk/railway/rsc.htm>
- <http://tube.fli.gov.uk/content/about/report/sqe/default.asp?exp=3> London Underground System Safety Case

For information on ALARP and SFAP try:

- <http://www.hse.gov.uk/hid/spc/perm09.htm>
- Worksafe Victoria MHAC Agenda Item 1.2.5 8th August 2001. Available from the Major Hazards Unit of Worksafe Victoria

Risk identification tools that can assist with Formal Safety Assessment (FSA) development include:

⁴ ALARP is used in the UK, but terms such as ALAP (as low as practicable), ALARA (as low as reasonably achievable) and SFAP (so far as practicable) are used by other pieces of legislation. It should be noted that these phrases have different meanings and put very different responsibilities on the operator of the facility. See Chapter 4.1.5 for further information on risk acceptability.

- Energy Barrier Analysis
- Consequence Analysis
- Preliminary Hazard Analysis (PHA), Hazard Analysis (HAZAN) or Workplace Risk Assessment and Control (WRAC)
- Fault Tree Analysis
- Event Tree Analysis
- Level of Protection Analysis (LOPA)
- Hazard and Operability Studies (HAZOP)
- Failure Mode and Effect Analysis (FMEA)

4.1.1.B. Risk or Hazard Register development

The Objective of creating a Risk or Hazard Register is to prepare a document that lists, outlines and prioritises the risks in an operation or organisation. As such it is an exposure document intended to communicate and monitor the current status of priority risks on the site. Normally, communication is the primary intention of a Risk Register. Obviously, regular review of the Risk Register is important due to changes in exposure over time and possibly a better understanding of the hazards and consequences. (hazards change, methods change, etc.).

The inputs to a Risk or hazard Register may come from a wide variety of sources including:

- Major Hazards from risk analysis studies
- Information from Safety Case
- Information developed through Management of Change
- SHE Hazards from
 - Incident Reports
 - Hazard reports
 - Job Safety Analyses (JSA's)
 - Audit Reports
 - Inspection Reports
 - Reviews

Potential data for the Hazards Register is screened using a Risk Matrix and only those hazards rated as extreme, high or moderate risks are recorded. Low or negligible risks are expected to be tracked and resolved by local management systems.

A key part of the Hazard Register is hazard tracking and close out mechanisms.

A key deliverable from a risk/hazard report is a SHE Critical Activities List. This list is a summary of activities required to control each identified hazard. The activities may include:

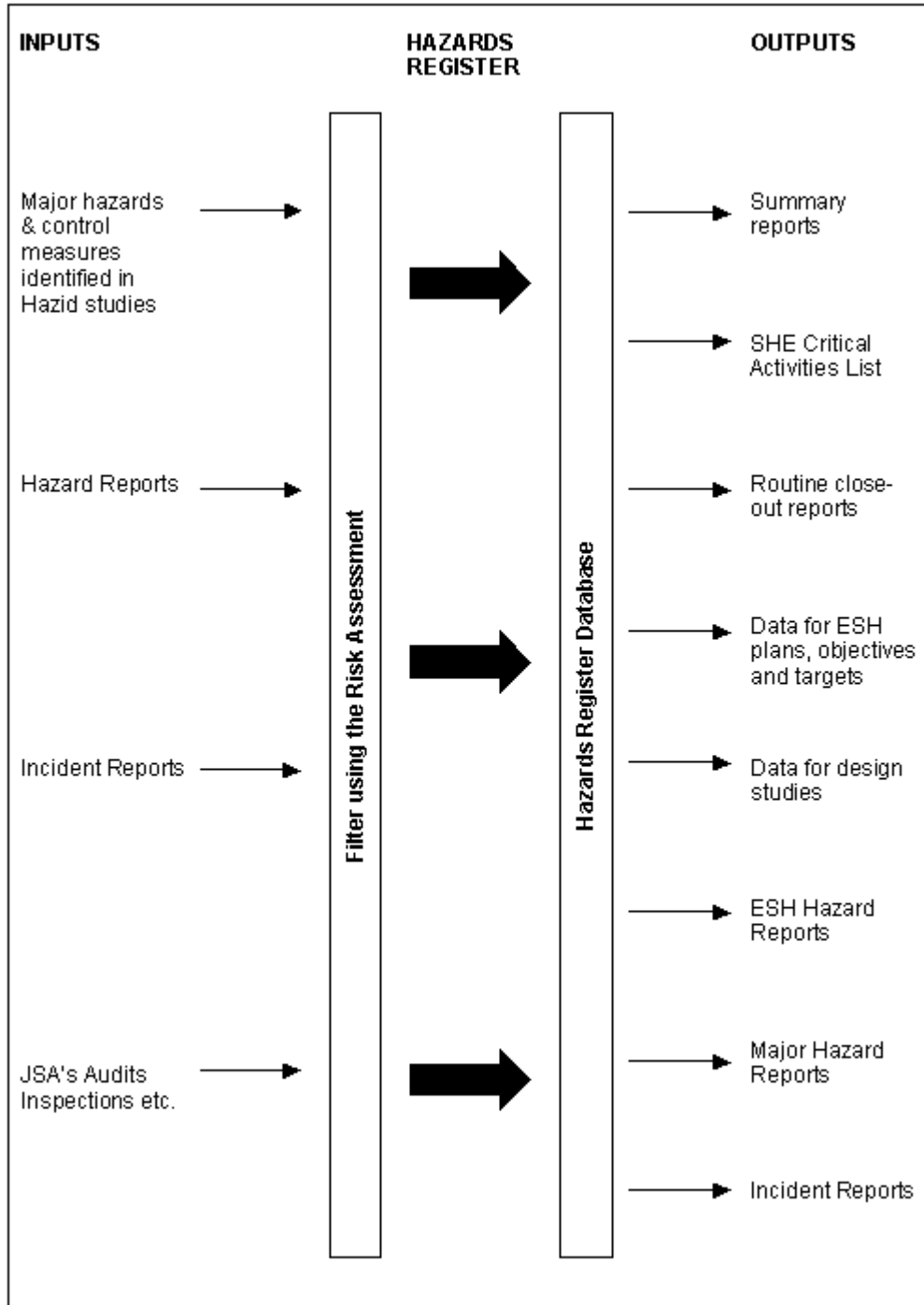
- A listing of control measures and performance measures
- Engineering changes

- Organisational and or procedural control
- Training and competence assurances
- Recovery measures

All activities will be assigned to individual responsibilities with an appropriate time frame.

In the Templates Appendix B is a sample page from a risk register (no 9). This page is formatted for a Safety Case and hence the description of control measures includes reference to the SMS, performance standard and COP (Critical Operating Parameter) as required by the guidelines for a SC. Regardless of the SC requirement, all risk registers need these if the control is critical.

Figure 4.1 Hazards Register Data Flow



This deliverable is referred to as “Broad Brush Risk Assessment (BBRA)” in the New South Wales MDG 1010 Guideline for Risk Management in the Minerals Industry. BBRA has been done in the minerals industry to identify a list of site risk management priorities.

Risk identification tools that can assist with preparation of a Risk or Hazard Register include:

- Consequence Analysis
- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Hazard and Operability Study (HAZOP)

For example, to explore more information on various approaches risk/hazard registers try:

- <http://www.planning.nsw.gov.au/plansforaction/mihaps-docs/mihaps-docs.html>
MIHAP paper no 3 Hazard Identification, Risk Assessment and Risk Control

4.1.1.C. Risk acceptability determination

The Objective of this deliverable is to decide if risks related to an issue, plan or system are acceptable. Determining risk acceptability involves initially determining the risk acceptance criteria. This is followed by some process of reviewing the issue, plan or system, establishing the relevant risks with controls in place and judging whether the relevant risks are or can be reduced to an acceptable level.

See Chapter 4.1.5 for further information on risk acceptability criteria.

For example, to explore more information on various Risk Acceptability approaches try:

- <http://www.iee.org/Policy/Areas/Health/hsb36.pdf>
- NSW Department of Urban Affairs and Planning, 1990. *Risk Criteria for Land Use Safety Planning*, Hazardous Industries Planning Advisory Paper No 4. ISBN 0 7305 71300. This useful resource is only available as a hardcopy. The publication can be purchased online (<http://www.planning.nsw.gov.au>) or alternatively contact the Department to order the publication.
- <http://www.planning.nsw.gov.au/plansforaction/mihaps-docs/mihaps-docs.html>
Paper No 3 Hazard Identification, Risk Assessment and Risk Control Section 7

Risk identification tools that can assist with determining the acceptability of a risk include:

- Consequence Analysis
- Preliminary Hazard Analysis (PHA), Hazard Analysis (HAZAN) or Workplace Risk Assessment and Control (WRAC)
- Fault Tree Analysis
- Event Tree Analysis
- Level of Protection Analysis (LOPA)
- CHAIR
- SIS

4.1.1.D. Identification of Critical Control Measures and Development of Performance Indicators

Control measures may be considered as the barriers between the inherent hazards of a facility and the realisation of an unwanted incident as a result of the hazards and ultimately the harm that may be caused to people, environment and equipment in the event of the unwanted incident. See section 4.1.5.1.b Quantitative Risk Analysis, Bow Tie Diagram as a pictorial representation of the overall system.

Control measures may be identified as part of the Hazard Identification process. For an existing facility a range of these measures would be readily identified both existing measures and possible alternatives.. The assessment of the effect of the measures on the hazard/outcomes needs to be determined for each hazard and outcome. The record for this could be usefully maintained in the Hazard Register and reviewed at agreed intervals.

It is important to determine which of the control measures are critical to the management of the facility, particularly if there are multiple control measures. The criticality of a measure has an important bearing on the maintenance frequency, test regime and management action if the measure has to be disabled. Some factors that might be considered that might indicate a critical control measure are:

- Control measure is relied on to control a number of different significant hazards
- Control measure is relied on to prevent the most likely cause of significant incidents.
- Control measure is relied on to reduce or mitigate incidents having potentially very severe consequences.
- Other control measures that provide backup are known to be of poor reliability or effectiveness
- There are a small number of barriers for a significant hazard.

All the control measures identified through the various hazard identification processes need to be assessed as to:

- Functionality ie does it control the hazard in the intended manner
- Survivability of the measure in an incident
- Reliability of the control, both individually and in combination with other controls
- Position in the hierarchy of control ie is the control at the least desirable end of the hierarchy or at a higher level.
- Independence and diversity. Can a set of controls be disabled by a single failure mechanism or does the failure of a control disable another?

For all control measures, a range of performance indicators is required, particularly for those controls deemed critical. The performance indicators measure both how well the controls are performing and how well the management system is monitoring and maintaining the controls. The performance indicators for control measures will generally relate to some standards or target levels of performance. The measures may be

qualitative or quantitative and may include absolute targets allowing no deviation or targets which may have scope for limited tolerable deviation.

Some Control Measures

Proactive:

These can also be subdivided into elimination of the hazard and prevention of realisation of the hazard.

- Design standards
- Mine Planning
- Safe operating procedures
- Inspections
- Ignition source control
- Berms
- Ventilation systems
- Isolation Systems
- Physical barriers
- Skills and Training
- Monitoring height of muck heap above drawpoints
- Monitoring of Air gap
- Roof bolting
- Fall restraint
- Remote bogging
- Change management process

Reactive:

These can also be sub divided into reduction of the consequence and mitigation of the consequence.

- Provision of fresh air base underground
- Emergency planning
- Fall harnesses
- Fire protection
- Oxygen breathing sets
- Relief valves
- Gas detection system
- Permit to work

For example, to explore more information on various control measures approaches try:

- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN10.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN10.pdf)
- <http://www.planning.nsw.gov.au/plansforaction/mihaps-docs/mihaps-docs.html>
MIHAPS Paper No 3 Hazard Identification, Risk Assessment and Risk Control
Section 6

4.1.1.E. Information for major or principal hazard plans

When the Objective or the intended deliverable is to supply information for Major or Principal Hazard Management Plans, the intention is to analyse and assess risks related to potentially high consequence hazards, as well as identify key controls. Major or Principal Hazard Management Plans are regulatory requirements in some Australian states for various mining hazards such as spontaneous combustion and gas drainage in underground mines.

These Plans are intended to be carefully developed documents that outline the management system in place to ensure the risks related to the specific major hazard are acceptable. Originally these plans were derived for hazards where uncertainty about the nature or locations of the hazard was high, such as for outbursts, ground control, inrush, etc.

For example, to explore more information on various Major or Principal Hazard Management Plans approaches try:

Risk identification tools that can assist with determining the acceptability of a risk include:

- Energy Barrier Analysis
- Consequence Analysis
- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Fault Tree Analysis
- Event Tree Analysis
- Level of Protection Analysis (LOPA)
- SIS

4.1.1.F Assessment of Safety Instrumented Systems (SIS) *

This section discusses the integrity of programmable electronic systems that are now extensively used in controlling remote operated equipment and processing plant in the mining industry. The article provides the necessary background for a basic understanding of a control that has often been seen as a black box that will always perform as defined. Reality is very different and the approach that should be used for assessing such systems and the applicable standards are covered. It is, as with all such processes that require a real understanding of the underlying theory, not to be undertaken without specialist assistance.

Functional Safety

Functional Safety is defined as the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. When the functional safety is achieved by safety instrumented systems, these systems will have to relate to the

* Section 4.1.1.F was provided by Dr Kyoumars Bahrami kyoumars.bahrami@worleyparsons.com
Principal Reliability & Risk Consultant – WorleyParsons Safety & Risk Management WorleyParsons, Melbourne

requirements set out in the standards AS/IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) or AS/IEC 61511 (Functional Safety of Safety instrumented systems for the process industry sector).

Protection Layers

Modern industrial processes tend to be technically complex, involve substantial energies, and have the potential to inflict serious harm to persons or property during a mishap (see also section 5.8 Identifying new controls or barriers).

The AS/IEC 61508 standard defines safety as “freedom from unacceptable risk”. In other words, absolute safety can never be achieved; risk can only be reduced to an acceptable level.

Safety methods to mitigate harm and reduce risk include:

- Changing the process or mechanical design, including plant or equipment layout
- Increasing the mechanical integrity of equipment
- Improving the basic process control system (BPCS)
- Developing additional or more detailed training procedures for operations and maintenance
- Using a safety-instrumented system (SIS)
- Installing mitigating equipment to reduce harmful consequences; for example, explosion walls, foams, impoundments, and pressure relief systems

The above safety methods are also called layers of protection or independent protection layers – **IPL** (see section 4.1.5.1.b Quantitative risk analysis - Level of Protection Analysis - LOPA).

The effectiveness of a protection layer is described in terms of the probability that it will fail to perform its required function when called upon to do so (a demand), and the scenario continues towards the undesired consequence despite the presence of the protection layer. This is called the *probability of failure on demand* (PFD). In the case of a SIS the PFD is described and categorised by a Safety Integrity Level (SIL). See also Appendix B. General format of LOPA Template.

LOPA is a one of the recognized techniques that is used by WSRM for selecting the appropriate safety integrity level (SIL) of the safety instrumented functions (SIF) per the requirements of the functional safety standards.

The following diagram, Figure 4.2, demonstrates the effect of adding independent layers of protection to the process to mitigate or reduce consequences of an unwanted event.

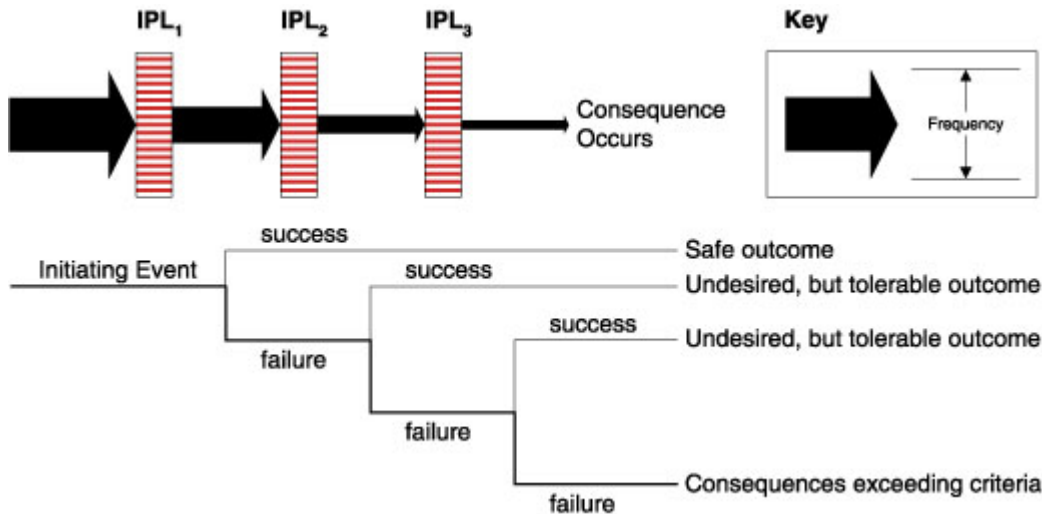


Figure 4.2. LOPA Process Diagram

Management of Functional Safety

Functional safety assessment is the critical activity that ensures functional safety has actually been achieved. Those carrying out the functional safety assessment shall be competent, shall have adequate independence and shall consider the activities carried out and the outputs obtained during each phase of every lifecycle and judge the extent to which the objectives and requirements of AS/IEC 61508 & 61511 have been met.

During the past few decades, systems and instrumentation vendors have developed sophisticated safety instrumented systems (SIS) to shut down potentially dangerous out-of-control processes before they do damage and to help plant personnel identify potential sources of these problems. Whereas basic process control systems (BPCS) control the making of on-spec product, SISs are intended to protect people, product and the environment by enabling a safe shutdown of the process if control is lost.

Protecting personnel, plant assets and communities starts with a properly designed safety instrumented system.

A well-designed SIS not only reduces risks from out-of control processes; it can also help users meet regulatory demands. A well-designed system can also increase plant availability by reducing the number of spurious “trips” caused by an SIS that fails to properly evaluate a safety situation and unnecessarily shuts down a process.

Standards and Safety-Related Concepts

Two new performance-based international standards govern the design and implementation of safety instrumented systems. The International Electrotechnical Commission’s (IEC) standard commonly referred to as IEC 61508, is targeted at suppliers of safety-related equipment and defines a set of standards for functional safety of electrical/electronic/programmable electronic safety-related systems.

Safety standard AS/IEC 61508 is quickly becoming a major deciding factor for purchasing process instrumentation for safety applications. This standard directs the processes used through the entire life cycle of a product, from the earliest stages of concept and design, through the manufacturing and final decommissioning of the product. AS/IEC 61508 provides industry with an effective means to quantify process risk and offers direction for proper design and manufacturing.

Another standard, AS/IEC 61511, is aimed at safety system users. The standard comprises formally collected best safety practices and addresses all safety life-cycle phases from initial concept, design, implementation, operations and maintenance modification, through to decommissioning.

The AS/IEC standards include several concepts that are vital to determining the level of risk in a plant and selecting an SIS that can meet the facility's safety needs. The first of those concepts is Safety Instrumented Function (SIF), which is defined as a single set of actions that protects against a single specific hazard. Each Safety instrumented system is comprised of one or more SIFs.

AS/IEC 61508, Parts 1–7

The AS/IEC 61508 standard, "Functional Safety: Safety Related Systems," is an international standard designed to address a complete SIS for the industries. The standard introduces the concept of a safety life cycle model to illustrate that the integrity of an SIS is not limited to device integrity, but is also a function of design, operation, testing, and maintenance. The standard includes 4 SILs that are indexed to a specific probability-to-fail-on demand (PFD). A SIL assignment is based on the required risk reduction as determined by a PHA.

AS/IEC 61511, parts 1–3

The AS/IEC 61511 standard, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector," is an international standard designed to be used as a companion to AS/IEC 61508. AS/IEC 61508 is intended primarily for manufacturers and suppliers of devices, whereas, AS/IEC 61511 is intended for SIS designers, integrators, and users in the process-control industry.

SIS Safety Lifecycle

Most certifications primarily address the end product. AS/IEC 61508, however, is process based and, therefore, encompasses all activities involved in the implementation of safety-related systems. Such activities begin with the concept phase of a project and finish when all of the electric, electronic, programmable electronic safety-related systems, other technology safety-related systems, and external risk-reduction facilities are no longer available for use.

WSRM uses the safety lifecycle concept, per AS/IEC 61508 & 61511, that describe the sequence of activities involved in the implementation of a SIS from conception through decommissioning.

Once the process risks are identified and existing protection layers are evaluated, an SIS is implemented to reduce the process risks to a tolerable level. Once installed, the SIS must be functionally tested on some specific frequency per the Safety Requirements Specification (SRS) and the calculated Safety Integrity Level (SIL) requirements.

The safety life cycle steps are as follows:

1. Perform conceptual process design
2. Perform PHA and risk assessment
3. Apply non-SIS protection layers to prevent identified hazards or reduce risk
4. Determine if an SIS is required
5. Define target SIL
6. Develop safety requirements specification (SRS)
7. Perform SIS conceptual design and verify that it meets the SRS
8. Perform SIS detail design
9. Perform SIS installation, commissioning, and pre-start up acceptance test
10. Establish operation and maintenance procedures
11. Perform pre-start up safety review (assessment)
12. Perform SIS start up, operation, maintenance, and periodic functional testing
13. Modify SIS (if necessary) by following a management of change procedure
14. Decommission SIS

Process hazard and risk assessment

AS/IEC 61508 & 61511 dictate that a process hazards analysis (PHA) be used to identify potential hazards in the operation of a process and to determine the protective measures necessary to protect workers, the community, and the environment. The scope of a PHA may range from a very simple screening analysis to a complex hazard and operability study (HAZOP).

A HAZOP provides a prioritized basis for the implementation of risk mitigation strategies, such as SISs.

If a PHA determines that the mechanical integrity of a process and the process control are insufficient to mitigate the potential hazard, an SIS is required. An SIS consists of the instrumentation or controls that are installed for the purpose of mitigating a hazard or bringing a process to a safe state in the event of a process upset.

Allocation of safety functions to protection layers

Safety Instrumented Systems (SISs) are subject to requirements based on the international standards AS/IEC61508 & 61511. Worley Safety and Risk Management offers assistance in identifying relevant requirements, carrying out necessary assessments and preparing required documentation.

Safety instrumented systems

Safety systems are designed to respond to conditions of the plant, which may be hazardous in themselves or, if no action were taken, could eventually give rise to a hazard. They must generate the correct outputs to prevent the hazard or mitigate the consequences.

SISs are also called:

ESD: Emergency safety Shutdown

SIS: Safety Instrumented (or interlock) System

BMS: Burner Management System
F&G: Fire and Gas system

The basic elements of a SIS include all parts from the sensor to the actuator, including inputs, outputs, power supplies and logic solvers:

1. Sensors, which monitor the state of an ongoing process (temperature, pressure, level, vibration,...).
2. Logic Solvers, which collect and analyse data from the sensors to determine whether emergency conditions exist, and how to respond (e.g., ignore, initiate a "safe" shutdown of the process, etc.). Typically, these are safety-rated electronic controllers.
3. Final Control Elements. Typically, these are pneumatically actuated valves, motors, ...

The purpose of Safety Instrumented Systems (SIS) is to take the process to a safe state when predetermined conditions are violated, such as set points for pressure, temperature, level, etc.

SIS Factors

According to the AS/IEC 61508 standard, the scope of an SIS is restricted to the instrumentation or controls that are responsible for bringing a process to a safe state in the event of a failure. The availability of an SIS is dependent upon:

- Failure rates and modes of components
- Installed instrumentation
- Redundancy
- Voting
- Diagnostic coverage
- Testing frequency

The SIS consists of the instrumentation or controls that are installed for the purpose of mitigating the hazard or bringing the process to a safe state in the event of a process upset. A SIS is used for any process in which the process hazards analysis (PHA) has determined that the mechanical integrity of the process equipment, the process control, and other protective equipment are insufficient to mitigate the potential hazard.

SIS safety requirement specification (SRS)

An SRS consists of safety functional requirements and safety integrity requirements; it is a collection of documents or information.

Safety functional requirements specify the logic and actions to be performed by an SIS and the process conditions under which actions are initiated. These requirements include such items as consideration for manual shutdown, loss of energy source, etc.

Safety integrity requirements specify a SIL and the performance required for executing SIS functions. Safety integrity requirements include:

- Required SIL for each safety function
- Requirements for diagnostics
- Requirements for maintenance and testing
- Reliability requirements if the spurious trips are hazardous

Safety Instrumented Function probability of failure on demand / Safety-Integrity Levels

The AS/IEC 61508 & 61511 standards require that companies assign a target safety integrity level (SIL) for all safety instrumented systems (SIS) applications. The assignment of the target SIL is a decision requiring the extension of the process hazards analysis (PHA). The assignment is based on the amount of risk reduction that is necessary to mitigate the risk associated with the process to an acceptable level. All of the SIS design, operation, and maintenance choices must then be verified against the target SIL.

The international standard AS/IEC 61508 defines four safety integrity levels (SIL1 to 4) to statistically represent the integrity of the safety instrumented system (SIS). They are defined as the measure for the safety performance of electrical or electronic control equipment.

An SIL takes into account device integrity, architecture, voting, diagnostics, systematic and common-cause failures, testing, operation, and maintenance. An SIL establishes an order of magnitude target for risk reduction. This target failure measure is the intended probability of dangerous mode failures to be achieved with respect to the safety-integrity requirements. The failure is specified in terms of either the average probability of failure to perform the design function on demand (for a low demand of operation) or the probability of a dangerous failure per hour (for a high-demand or continuous mode of operation). The higher the SIL, the greater the impact of a failure and, therefore, the lower the failure rate that is acceptable.

A SIL can be considered a statistical representation of the availability of an SIF at the time of a process demand. A SIL is the litmus test of acceptable SIS design and includes the following factors:

- Device integrity
- Diagnostics
- Systematic and common cause failures
- Testing
- Maintenance

In modern applications, a programmable electronic system (PES) is used as the core of a SIS.

Safety Integrity Levels Table

Table 4.3. Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to $\leq 100,000$
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to $\leq 10,000$
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100

Table 4.4. Safety integrity levels: frequency of dangerous failures per hour

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	Frequency of Dangerous Failures Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

The Probability to Fail on Demand is a statistical measurement of how likely it is that a process, system, or device will be operating and ready to serve the function for which it is intended. Among other things, it is influenced by the reliability of the process, system, or device, the interval at which it is tested, as well as how often it is required to function. Below are some representative sample PFD values. They are order of magnitude values relative to one another.

Selection of a Safety Integrity Level

A vital first step in the safety lifecycle is that the necessary safety functions are derived from an analysis of the hazards and risks. If a PHA concludes that an SIS is required, AS/IEC 61508 requires that a target SIL be assigned. Safety Integrity Levels or SILs define the levels of protection – amount of risk reduction needed for a particular SIF. The IEC standards describe four possible discrete SILs.

The assignment of a SIL is a corporate decision based on risk management and risk tolerance philosophy. Safety regulations require that the assignment of SILs should be carefully performed and thoroughly documented. Completion of a HAZOP determines the severity and probability of the risks associated with a process.

It is not only the safety integrity of the safety functions that is important, but also the effective and correct specification of the safety functions themselves.

Once the SIL level of a given SIF has been calculated, the standard defines the acceptable probability of failure on demand (PFD) of the associated SIS. A SIF with a high SIL rating will require the use of a low system with a low average PFD. An important factor in determining the PFD is the frequency of system testing, including the stroking of its valves. The longer the time between tests, the higher the PFD.

Several methods of converting HAZOP data into SILs are used. Functional safety standards provide information on a number of different methods that enable the safety integrity levels for the safety instrumented functions to be determined, among those are:

- semi-quantitative methods – calibrated risk graph,
- the safety layer matrix,
- qualitative methods – risk graph,
- layers of protection analysis.

Company standard SIL selection method

Any Safety Integrity Level selection method adopted by a company needs to be easy to use and yield results quickly. A labour intensive and time-consuming SIL selection method will surely be abandoned when companies attempt to apply the method to the hundreds or thousands of SIF evaluations that they will need to perform. Thus, to make the procedure easier to utilize, it is recommended that companies develop a database file that standardizes the procedure to be followed.

WSRM has recently developed a very user friendly database file with the goals of compliance with applicable regulations, consideration of the practices of industrial peers, conformance with the recommendations of applicable standards, and consistence with each facility risk ranking schemes that can be used to select SILs.

If such a company tuned databases were used, then it would allow multiple remote plant sites to quickly, efficiently and consistently evaluate SIL requirements for their Safety Instrumented Systems. This would allow facilities to make sound business decisions regarding the risks associated with their plant.

Reliability analysis / Quantitative methods for Verification of safety integrity levels

One of the activities that should be performed according to the international functional safety standards is the SIL verification for a Safety Instrumented Function. The first step in such a SIL verification or reliability analysis is the selection of a reliability analysis technique. Secondly input data should be gathered. These first two steps can be major hurdles to be taken. This calls for automated quantitative methods and tools that can easily perform these reliability analyses.

The quantitative methods can be utilized to select the appropriate Safety Integrity Level associated with Safety Instrumented Systems. Selection of an overly conservative Safety Integrity Level can have significant cost impacts. These costs will either be associated with increased Safety Instrumented System functional testing or complete removal / upgrade of the existing Safety Instrumented System. In today's highly competitive business environment, unnecessary costs of any kind cannot be tolerated.

Furthermore the results of a reliability analysis should not only express the PFDavg value of a specific Safety Instrumented Function, but also focus on availability numbers, as end users often also require these numbers. In addition to the PFDavg value from which a Safety Integrity Level is derived, there are also requirements based on the architectural constraints concept that need to be considered. Along with other issues like variable proof test intervals for different parts of the Safety Instrumented Function there is a need for automated tools that can help during a SIL verification assessment.

Worley safety and risk management has developed a guideline for SIL verification in line with the functional safety standards and is using state of the art automated tools to carry out the task.

The appropriate testing for an SIS is a key to insure safety availability requirements are satisfied.

The quantitative method to determine the frequency of testing is the accepted approach by most companies. Reliability engineers generally use one or more of the following methods:

1. Markov Models
2. Reliability Block Diagrams
3. Fault Tree Analysis (FTA)

Markov modelling is a very complex, but exact, method for determining the availability of logic solvers. It is not recommended for the entire SIS or even a single loop calculation. The complex transition diagrams and matrix math can elevate the difficulty of a precision calculation of an entire SIS.

Reliability block diagrams are the reciprocal in complexity to Markov Models in that the block diagrams are too simplistic. The block diagrams can't handle test intervals or repair times and therefore are almost useless in calculating test frequencies.

By far the best and most accepted method for the entire SIS or even a single loop, is the *fault tree analysis*.

FTA is useful for a large SIS with many components or just a single loop.

LESSONS LEARNED 4.1

Before quantitative methods e.g. fault trees or Markov Models were utilized, companies used an "experienced" approach. The experienced method merely set the testing frequencies on what has worked before regardless of the architecture or number of components in the SIS.

The disadvantage of the experienced approach is that a company could be testing too frequently or not frequent enough because no adjustment is made for SIS complexity or number of components. The quantitative method has shown us that architecture, redundancy, and number of devices, has a significant affect on probability to fail on demand and therefore testing frequency requirements.

Example for SIL Verification – Sample Calculations

The following sample calculation shall be performed for a single Safety Instrumented Function for a Safety Instrumented System to document the ease in which one can calculate the required Safety Integrity Level.

Consider the following physical block diagram for a safety instrumented function:

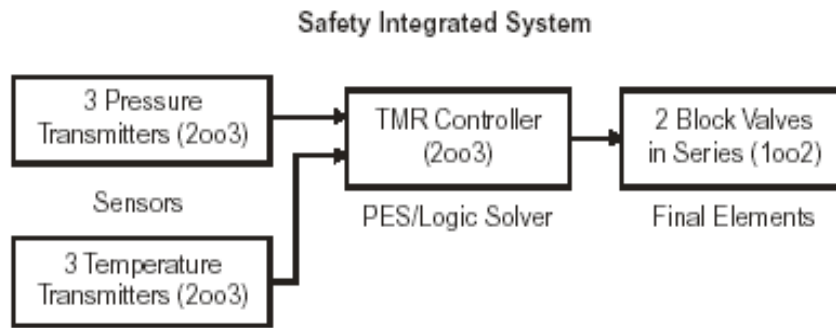


Figure 4.5. Architecture of the example

The equations given in AS/IEC 61508 can be used to calculate PFD_{avg} for sensors (2oo3) and block valves - final elements (1oo2) in series.

Then, the following equation may be used to calculate PFD_{avg} for the whole system:

$$\text{System PFD}_{\text{avg}} = \text{Sensors PFD}_{\text{avg}} + \text{Block Valves PFD}_{\text{avg}} + \text{Controller PFD}_{\text{avg}}$$

Using the AS/IEC 61508 equations and the automated tools will result in the following table:

Table 4.6 SIL verification calculation results

	λ^{DU}	TI	PFD	Result
Pressure Transmitters (2oo3)	2.28E-06	4380	1.00E-04	
Temperature Transmitters (2oo3)	2.85E-06	4380	1.56E-04	
Total for Sensors				2.56E-04
Block Valves – Final element (1oo2)	2.28E-06	4380	3.33E-05	
				3.33E-05
Tricon Controller (Logic solver)	2.00E-05			

PFD _{avg} for System				3.09 E-04
-------------------------------	--	--	--	-----------

To determine the SIL, compare the calculated PFD_{avg} to the Table 4.3 figures. In this example, the system is acceptable as an SIS for use in SIL3 applications.

References

To explore more information on SIS try following internet addresses:

- <http://www.sts-aiiche.org/cast1202/>
- <http://www.hcasia.safan.com/mag/hoct03/it46.pdf>
- <http://www.triconex.com/NR/rdonlyres/34D43700-882E-4D36-B01C-97B8D2E0DBF6/0/PCSTechnicalPaperTestingandByPassingSafetyInstrumentedSystems.pdf>
- http://www.itk.ntnu.no/ansatte/Onshus_Tor/IEC61508/Guideline%20IEC%2061508%20rev%2013-10-00.pdf
- <http://www.sensorsmag.com/articles/1004/33/main.shtml>
- <http://www.aesolns.com/articles/lss.pdf>
- http://www.miinet.com/approvals/what_is_61508.pdf
- <http://www.bently.com/articles/apnotes/an149409.pdf>
- <http://shop.era.co.uk/products.asp?recnumber=193>
- http://www.isa.org/InTechTemplate.cfm?Section=Article_Index&template=/Content
- <http://www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm>
- <http://www.ce-mag.com/archive/04/Armstrong.html>
- <http://www.automationtechies.com/sitepages/pid1071.php>
- http://www.us.tuv.com/product_testing/related_articles/semi_safety.html
- <http://www.nswmin.com.au/ohs/smhb2002/burgess.shtml>
- <http://www.hotkey.net.au/~mjbauer/ACS-SCS%20Paper.htm>
- http://www.multiplan.co.ae/sil_assessment.htm

For information on functional safety and related issues try:

1. IEC Standard 61508, 1998, IEC publications.
2. IEC Standard 61511, 2003, IEC Publications.
3. Off Shore Reliability Data, 2002, Det Norske Veritas, OREDA Publications.
4. Smith, D. J, "Reliability, Maintainability, and Risk – Practical Methods for Engineers", Butterworth-Heinemann, Sixth Ed., pp. 263- 272 (2003)
5. Center for Chemical Process Safety of the American Institute of Chemical Engineers, "Guidelines for Process Equipment Reliability Data", AIChE/CCPS, pp. 211-212 (1989).
6. Center for Chemical Process Safety of the American Institute of Chemical Engineers, "Layer of Protection Analysis, A Simplified Process Risk Assessment".

4.1.1.G. Information for Operational Guidelines

The Objective of this deliverable is to generate information that can be used to help derive guidelines for operating. Operational Guidelines provide the detail for specific tasks. Operational Guidelines are information involving a group of related tasks such as overburden dump operation, drill and blast operation, longwall operation, processing equipment overhaul, exploration site operation, etc. As such it is guidance for a team or group of operators concerning the objective of that work group.

Risk identification tools that can assist with development of information for Operational Guidelines include:

- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Human Error Analysis (HEA)
- Hazard and Operability Study (HAZOP)

4.1.1.H. Information for maintenance plans or guidelines

The Objective of this deliverable is to produce information for Maintenance guidelines, similar to that discussed above under “Operational Guidelines” or for reviewing and setting priorities in Maintenance Planning. The latter may be similar to Reliability Centred Maintenance where maintenance resources are focussed on key reliability (high risk) areas.

For example, to explore more information on various Reliability Centred Maintenance approaches try:

- http://www.mishc.uq.edu.au/publications/TR_Hunter_Valley.pdf

Risk identification tools that can assist with development of information for Maintenance Plans or Guidelines include:

- Preliminary Hazard Analysis (PHA), Hazard Analysis (HAZAN) or Workplace Risk Assessment and Control (WRAC)
- Fault Tree Analysis (FTA)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- Human Error Analysis (HEA)
- Level of Protection Analysis (LOPA)

4.1.1.I. Hardware design review

The Objective of this deliverable is to review a proposed mobile, fixed, process, portable or other equipment design to produce information identifying key risk control features and any potential equipment design risks, usually with recommended new controls to address those risks.

For example, to explore more information on various Hardware or safety design approaches try:

- <http://www.hq.nasa.gov/office/codeq/risk/rmt.pdf>

Risk identification tools that can assist with development of Hardware Design Review Recommendations include:

- Hazard and Operability Study (HAZOP/CHAZOP)

- Failure Modes, Effects and Criticality Analysis (FMECA)
- Human Error Analysis (HEA)
- SIS

4.1.1.J. Option / selection review

Sometimes it is necessary to compare optional designs or methods where risk forms one of the criterion for option selection. The Objective of this deliverable is to generate information that identifies the risks in each option and allows comparison. The latter is greatly affected by the risk analysis or calculation method.

Effective option evaluation requires quantitative risk analysis or, if risk ranking is the **only** option, a carefully structured comparison framework and the use of non-parametric statistics to demonstrate differences.

 Risk ranks should not be added, averaged and compared to choose options. Ranks are only relevant for ordering risks. **THIS IS A KEY ISSUE.**

LESSONS LEARNED 4.2

A mine decided to compare one potential piece of new equipment to an option. They applied risk assessment methods to both, identifying a set of potential unwanted events with semi-quantitative risk ranks for each. After the exercises, they created an average risk rank for each piece of equipment, assuming that the lowest average risk rank would be the best option. Their assumption may be incorrect.

Risk identification tools that can assist with Option Review include:

- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Human Error Analysis (HEA)

4.1.1.K. Review of change management plan

The Objective of this deliverable is identification of threats to the success of a planned change and / or process of change. Change Management is a major part of any successful business. Significant change can involve risks to many areas of the business. Therefore the objective would be to identify and assess the risk inherent in the change, providing priority risk based controls for integration into the Change Management Plan.

For example, to explore more information on various Change Management approaches try:

- <http://www.ncrel.org/sdrs/areas/issues/educatrs/leadrshp/le5spark.htm>

- http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html
- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN28.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN28.pdf)
- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_maj_haz_interest/\\$File/Griffiths.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_maj_haz_interest/$File/Griffiths.pdf). This is the first of a number of papers discussing management of change.
- Centre for Chemical Process Safety, 1989. *Guidelines for Technical Management of Chemical Process Safety*. ISBN No: 0816904235. This useful resource is only available as a hardcopy. The publication can be purchased online (<http://www.aiche.org/ccps/products/titledtl.asp?recpt=12&BN=0-8169-0423-5>) or alternatively contact the Centre to order the publication.

Risk identification tools that can assist with change management plan review development include:

- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Human Error Analysis (HEA)
- Fault and Event Tree Analysis
- Hazard and Operability Study (HAZOP/HAZOP)
- SIS

4.1.1.L. Information for drafting of Standard Operating Procedures (SOPs)

The Objective of this deliverable is to produce information on hazards and required controls for inclusion in the drafting of a Standard Operating Procedure (SOP). Once a site has identified a required SOP, risk assessment is done to review the current or planned job steps to identify hazards and controls.

For example, to explore more information on various Standard Operating Procedures (SOPs) approaches try:

- <http://www.usfa.fema.gov/downloads/pdf/publications/fa-197.pdf>

LESSONS LEARNED 4.3

Many mines have adopted the form used for reviewing risks in a procedure (the Job Safety Analysis form) as the format for Standard Operating Procedures (SOPs). Although the form can be used to display useful information, the JSA form was not intended for this purpose.

SOPs should be documented in a user-friendly manner considering understand ability (number and size of words), use of jargon, visual ease of use, inclusion of graphics / illustrations, etc.

As a guide, an effective SOP is one that can be flowcharted. If the flowchart cannot be fitted on one page is an indication that more than one procedure is being covered.

Risk identification tools that can assist with drafting SOPs include:

- Job Safety or Hazard Analysis (JSA / JHA)
- Preliminary Hazard Analysis (PHA)
- Hazard Analysis (HAZAN)
- Workplace Risk Assessment and Control (WRAC)
- Hazard and Operability Study (HAZOP/CHAZOP)
- SIS

4.1.1.M. Informal risk awareness on day-to-day tasks

The Objective of this deliverable is to create a state of risk awareness in the minds of individuals about to undertake a task or during a task where an unexpected change has occurred. Many mines have adopted “mental models” to prompt people to think about the risks.

Examples of Risk identification tools for Day-to-Day Risk Awareness include:

- “PLAN”,
- “Stop & Think”
- “Hudson’s Rule of Three”
- “Stepback 5*5”
- “Positive Attitude Safety System (PASS)”
- “Take 5”
- “Buddy System”
- “SLAM” Stop, Look, Assess and Manage

See Appendix C for an example of two of the tools.

4.1.2 Identifying and describing the system to be reviewed

It is important to put boundaries around the system (i.e. the task, the process, the design, the geographical area, etc.) that is to be reviewed using risk assessment. Boundaries define what the risk assessment covers, reducing the likelihood of overlaps or gaps. Setting the systems boundaries also helps to identify the information required for the risk assessment.

Some examples of system boundaries for the deliverables mentioned before are as follows:

Table 4.7 Some examples of system boundaries for the expected deliverables

<i>Deliverable</i>	<i>Example System Boundary</i>	<i>Potential System Information Sources for the RA</i>
Formal Safety Assessment development	The mine or plant site fence line plus related off-site activities	Site plan, business process map, design criteria, engineering documents, P&I diagrams, plant & equipment design info, etc., relevant regulations and Standards, incident history, external influences.
Risk or Hazard Register development	The mine or plant site fence line plus related off-site activities	Site plan & site business process map, external influences
Risk acceptability determination	The specific process or system where the risk issue exists	Details on the processes or systems (depends on nature of system – hardware, procedure, etc.)
Identification of Critical Control Measures/Performance Indicators	Specific hazard identified in Hazard Identification Process	Fault Tree showing development of hazard to an unwanted event. Controls identified during Hazid Facility data on effectiveness, etc of control Incidents related to specific hazard
Information for major or principal hazard plans	The processes or systems where the hazard is located	Process maps or other information on the processes or systems where the hazard is located, relevant regulations and Standards, incident history, external influences
Information for operational guidelines	The specific operation from start to finish	Details of the current operation such as a process map, relevant regulations and Standards, incident history
Information for maintenance plans or guidelines	The specific system that is to be maintained	Details of the current operation such as a process map or the current maintenance plan, maintenance manuals
Hardware design review	The hardware or process components from the start to the finish of the system	Component illustrations, Process and Instrumentation Diagrams (P&I diagrams) or other design illustrations, operating specifications
Option/selection review	The systems where the options will have an affect	Details on each option and the systems where they might operate (depends on nature of system – hardware, procedure, process map etc.), feasibility documents
Review of change management plan	The change process from start to finish	Potential Change Management Plan detail and relevant other information depending on the nature of the change
Information for drafting of SOPs	The task from start to finish	Current work practice steps, operating practice manuals, incident history, regulations, codes of practice & Standards
Informal risk awareness on day-to-day tasks	The task at hand from start to finish	Individuals image of the task at hand, work instruction documents, external influences

4.1.3 Identifying and understanding the potential hazards

Risk Identification is “ the process of determining what can happen, why and how” (AS/NZS 4360:1999). To identify risks we must understand the hazards.

The quality of a risk assessment greatly depends on the recognition that:

Firstly – identify and understand the hazards

Secondly – identify the unwanted events and assess the specific risks



THIS IS A KEY ISSUE.



If the existence, nature or potential consequences of a hazard are not reasonably certain, the risk assessment should not proceed. **THIS IS A KEY ISSUE.**

To identify and understand the hazards consider:

- **Hazard identification**

Identifying the existence and location of a potential source of harm or threat to the system objectives

- **Hazard assessment**

Determination of the magnitude / amount / size of the hazard and thereby its potential consequences, as well as identification of any uncertainties about the nature of the hazard (i.e. lack of certainty about its nature, size, consequences, etc.)

The risk assessment exercise will identify specific potential unwanted events or circumstances but, especially in complex or major assessments, it is helpful to define the types of hazards that will be considered during the Scoping process.

For example, before starting a risk assessment exercise involving chemicals, it may be desirable to establish the specific type or name of the chemical, the amounts of chemical to be considered (the magnitude of the hazard) and the general consequences of a problem with the chemical. Of course some of this information is available on the relevant MSDS. Similarly, “natural” hazards such as ground, gas in the workings, propensity to spontaneous combustion, inrush exposure, rainfall and others may need to be clarified before the risk assessment to ensure uncertainties are clarified.

A useful concept for helping to identify hazards in any system is to consider what energies are part of the system being considered. Energies exist in the Minerals industry because they are inherent in the conditions that exist and because they are brought into the workplace. All energy that has the potential to do harm is, by definition, a hazard. However work is done by controlling energies and it is lack of or insufficient control of energy that leads to some level of risk depending on the likelihood of release and the consequences. Energy sources are limited and the following covers virtually all:

- **Gravity:** is a naturally occurring energy which causes things or people to fall or move downhill. Includes roof/rib-back/sides, high/low wall, elevated equipment, and people working at heights.

- **Electrical:** includes all types and voltages of electricity from HV to batteries to induction, static.
- **Mechanical:** includes mobile equipment as well as moving parts on stationary equipment
- **Chemical:** energy in the form of gases, liquids, solids of which some are natural eg water, methane, coal whilst others are introduced eg acetylene, solvents, explosives, cyanide.
- **Pressure:** air, water, pneumatics, springs, gases are all possible stores of pressure energy-including accumulators
- **Noise:** is also a pressure energy but as the most significant compensated health issue is considered separately
- **Thermal:** Energy that comes from hot or cold surfaces
- **Radiation:** in the form of sun light or nuclear/isotope radiation
- **Body Mechanics:** includes the human bodies own energy to move which includes lifting, pushing, pulling, climbing, positioning
- **Biological:** covers the many sources of energy in other forms of life from wildlife to small viruses or bacteria

The listing is a prompt when working through identifying hazards for assessment, it provides an alternative frame of reference and increases the probability that hazards will not be overlooked.. The exact type of energy is not critical but recognition is, along with what it can do and the magnitude.

There is a set of Strategies for prevention and management of unwanted energy exchanges.

These were published by Haddon⁵. They are given with brief examples below:

No	Strategy	Examples
1	Prevent the marshalling of the energy	Remove dense growth of trees and undergrowth around facilities Don't climb to a height
2	Reduce the amount of energy marshalled	Reduce the speed of vehicles Have staggered ladders or stairs with platforms between
3	Prevent the release of energy	Ban ignition sources amongst flammable material Fit guard rails
4	Modify the rate of release or spatial distribution of the energy	Install pressure relief valves Wear safety line and harness while working on ladders
5	Separate the energy release and the susceptible structure in time or space	Zone industry away from residential areas (space) Use tagging/lock out procedures (time)
6	Separate the energy release from the susceptible structure by a barrier	Install guards Wear safety glasses

⁵ Haddon, W (1970) "On the Escape of Tigers – an Ecologic Note", Technology Review, vol 72 No 7, MIT, Mass

7	Modify contact surfaces involved	Remove corners and edges on table tops Ensure height of truck cabs and trays are different
8	Strengthen susceptible surfaces	Exercise muscles before starting work Fit ROP to vehicles
9	Detect, evaluate and counteract damage quickly	Install earth leakage relay Sprinkler systems, fire extinguishers
10	Optimise repair and rehabilitation	Light duties at work Specialist medical facilities

LESSONS LEARNED 4.4

Misunderstanding of hazards, not usually their existence but more commonly their nature and magnitude, has contributed to major or catastrophic incidents in the mining industry in the distant and recent past. In some cases, the hazard was identified but NOT understood so the specific risks were underestimated leading to inadequate controls and unacceptable residual risk.

One of the principal reasons that risks are underestimated is the failure to map all the potential contributors to an incident event and thereby clarify the interrelationship of the various modes of failure and event outcomes.

It may be helpful to create a Hazard Inventory Table for a complex or major risk assessment. In the Scoping stage, identify and note the hazard type, hazard locations and magnitude/amount of the hazard with or through discussion with the risk assessment client. Discussion and resolution of these areas will help establish the degree of uncertainty.

The development of a Hazard Inventory Table before the risk assessment exercise will help to ensure that the hazards are known and understood, not left to team assumptions. The table will also assist the future review of risk assessment reports by providing a clear image of the assumptions made about key hazards.

LESSONS LEARNED 4.5

There are many examples in the Australian minerals industry of changing hazards. In fact, hazards in the minerals industry probably change more than many other industries as we open new ground. In some cases risks have been assessed with the hazard assumed to be moderate but, over time, the hazards increased to a higher, even catastrophic, levels. The past risk assessment were not reviewed after the changes, controls were inadequate and losses occurred.

Example:

Table 4.8 Example Hazards Inventory Table for a Highwall Mining System (partial list)

<i>Hazard Type & Location</i>	<i>Magnitude of Hazard</i>	<i>General Nature of Consequences</i>
<i>CHEMICAL</i>		
Water (rainfall) in the overall working area.	Rainfall uncertainty is high so hazard defined as 1 in 100 year rainfall over catchment area. Large catchment area (10 km ² .) with high run off above the mining location	Rapid and violent flooding of the work area – major equipment damage, fatalities & major delays
Water (mine) – in the water used for cooling / sprays, etc.	Water pH varies up to 11 so manage as if all water is pH 11. All mine water could be affected	Moderate environmental damage, major equipment damage due to corrosion
Spontaneous combustion – in the coal left behind	Propensity to spon comb is unknown so assume that it can happen. At least 50-% of resources left behind and broken so major source	Fire and loss of project, explosion blasting working area
Diesel fuel stores at fuel depot in the work area. Possible underground supply pipelines	On site stores are up to 50,000 litres so manage as if 50,000 litres present. Is the pipeline design adequate or are leaks possible.	Moderate/major environmental damage, major fire.
Hazardous materials stored and used on site eg Cyanide, Ammonium Nitrate	Incorrect handling resulting in exposure to cyanide, contamination of ammonium nitrate	Fatality, fire, long term health damage
<i>GRAVITY / GEOLOGICAL</i>		
Highwall failure in working area	Highwall structures are known and face has been cleaned to reduce loose materials so moderate hazard. Likely max 1 tonne fall	Damage to protection over entry, fatal to persons outside protection near highwall
Working adjacent to significant drop off eg high wall or stope filling	Vehicle/equipment or personnel go over edge of high wall/stope	Damage to equipment, reduced production capability, fatality, serious injury
Ground support failure of access road	Road collapses under heavy truck, dozer or drag line	Major equipment damage, injury, fatality, production delays
Changes in access routes over a short period	Operators returning from leave unfamiliar with changes	Equipment damage, injuries, fatalities
<i>MECHANICAL</i>		
Mobile & fixed equipment in overall working area	Large front end loaders and haulage/water trucks all with access issues and poor visibility	Major equipment damage, fatality, major delays, interaction with other large and small mine vehicles, structural damage
<i>BIOMECHANICAL</i>		
Manual handling	Some heavy, awkward items in poor conditions, inadequate assistance provided	Major, long term injury, long term physical damage to workforce


As the table illustrates, the value of defining the hazard information is clarification before the risk assessment exercise. Clarification whether there is uncertainty such as that indicated in the CHEMICAL examples above. This approach helps the team more accurately and consistently consider the unwanted events (specific risks) and potential consequences.

Include this information in the report to communicate the assumptions that were made about the hazards.

Depending on the system being assessed, other sources of Hazard may need to be considered. The following are some sources of hazard:

Ground control	Remote controls	Commodity Classification
Airgap in block cave	Hydrology	Rock hang up in stopes
Ventilation	Crown pillar degradation	Equipment Operation
Commodity price	Inundation	Exchange rate
Rock falls	Inflation	Environment
Gas outbursts	Growth forecasts	Vehicle interactions
Cost/Capital deficit	Shaft Sinking	Shaft Winding
Cost overrun	Completion date exceeded	Slope stability
Tailing Dam	Operating Cost estimates	Commissioning time
Airborne Dust	Mine throughput	Diesel Particulates
Quality of product	Rock bursts	Market value of product
Seismic Activity	Soil/rock mass character	Fires/explosions
Explosives	Infrastructure location	Sodium Cyanide
Equipment Selection	Dangerous openings	Rock fragmentation
Temperature	Rock comminution	M/c people interaction
Mining method	Biological	Radiation
Biomechanical		

4.1.4 Selecting Risk Assessment Method – the Means of Systematically Identifying the Risks

 To identify the specific unwanted events select the appropriate Risk Identification method or tool. **THIS IS A KEY ISSUE**. It is important to match the Objective (Expected Deliverable, System & Issue) to the risk identification method or tool.

The following information identifies relevant methods or tools for the previously outlined deliverables, firstly by listing some of the relevant risk assessment techniques, then by suggesting the deliverables with which these can assist and, finally by providing links to good sources of further information on these techniques.

The most relevant risk assessment techniques from the suggested deliverables are as follows:

- **Informal RA** –(Team: local workgroup) general identification and communication of hazards and risks in a task by applying a way of thinking, often with no documentation. See Section 4.1.1.L and Appendix C

- **Job Safety / Hazard Analysis (JSA / JHA)** – (Team: Local workgroup) general identification of hazards and controls in a specific task, usually for determining the basis of a Standard Work Practice (SOP). See Appendix G
- **Energy Barrier Analysis (EBA)** –(Team: multi-disciplinary with facilitator) detailed analysis of determining phases of an events and control mechanisms. See Appendix G
- **Consequence Analysis** – (Team: multi-disciplinary with facilitator) general to detailed understanding of the magnitude of unwanted events with potential to apply quantitative analysis. See Appendix G
- **Preliminary Hazard Analysis / Hazard Analysis / Workplace Risk Assessment and Control (PHA / HAZAN / WRAC)** – (Team: varies depending on application, could be project team or local workgroup) general identification of priority risk issues / events, often to determine the need for further detailed study. See Appendix G
- **Hazard and Operability Study (HAZOP)** – (Team: Multidisciplinary team with facilitator) systematic identification of hazards in a processing design. See Appendix G
- **Fault Tree Analysis (FTA)** – Team: Analyst working with input from local workplace group) detailed analysis of contributors to major unwanted events, potentially using quantitative methods. See section 4.1.5.1.b
- **Event Tree Analysis (ETA)** – (Team: analyst working with data from local workplace group) detailed analysis of the development of major unwanted events, potentially using quantitative methods. See section 4.1.5.1.b
- **Failure Modes, Effects and Criticality Analysis (FMECA)** – (Team: facilitator with local workplace or project group) general to detailed analysis of component reliability risks. See Appendix G
- **Human Error Analysis (HEA)** – (Team: Analyst with input from local work group) general or detailed analysis of human factors or reliability issues. See Appendix G
- **Level of Protection Analysis (LOPA)** – (Team: LOPA specialist with input from multidisciplinary team) a special form of event tree that is optimised for determining the frequency of an unwanted event that can be protected by one or more independent protection layers. See Section 4.1.5.1.b

Table 4.9 Risk Assessment Tools for Potential Deliverables / Objectives

This table suggests the risk assessment techniques that can help achieve the previously discussed project or site deliverables.

Potential Deliverable / Objective	Informal RA	JSA / JHA	EBA	Conseq. Analysis	PHA / HAZAN / WRAC	HAZOP / CHAZOP	FTA	ETA	FMECA	HEA	LOPA	CHAIR	SIS
Formal Safety Assessment development			X	X	X	X	X	X	X	X	X		X
Risk or Hazard Register development				X	X								X

Potential Deliverable / Objective	Informal RA	JSA / JHA	EBA	Conseq. Analysis	PHA / HAZAN / WRAC	HAZOP / CHAZOP	FTA	ETA	FMECA	HEA	LOPA	CHAIR	SIS
Risk acceptability determination				X	X		X	X			X		X
Identification of Critical Controls/Performance Indicators				X	X	X	X	X			X		X
Information for major or principal hazard plans			X	X	X		X	X			X		X
Information for operational guidelines					X	X				X			X
Information for maintenance plans or guidelines					X	X	X		X	X	X		X
Hardware / processing design reviews						X			X	X			X
Option/selection review					X		X	X		X	X	X	X
Review of change management plan					X					X			X
Information for drafting of SOPs		X			X	X				X	X		X
Informal risk awareness on day-to-day tasks	X	X											

Informal Risk Assessment

- http://www.racingsmarter.com/safety_awareness_program.htm
- <http://passinc.net/components.html>

Job Safety or Hazard Analysis (JSA / JHA)

- <http://www.ccohs.ca/oshanswers/hsprograms/job-haz.html>
- http://www.acusafe.com/Hazard_Analysis/OSHA_JSA_3071.pdf
- <http://www.inel.gov/procurement/forms-documents/432-58-r4.pdf>
- http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_construction_jsa
- http://www.osha-slc.gov/SLTC/etools/oilandgas/job_safety_analysis_process.html

Consequence Analysis

- <http://www.sverdrup.com/safety/cause.pdf>

Preliminary Hazard Analysis (PHA) or Workplace Risk Assessment and Control (WRAC)

- <http://www.sverdrup.com/safety/pha.pdf>
- http://www.safeware-eng.com/software-safety/prelim_analysis.shtml

Hazard and Operability Studies (HAZOP)

- http://www.mep.tno.nl/wie_we_zijn_eng/organisatie/afdelingen/industriële_veiligheid/productbladen/productblad_IV_HAZOP_eng.html
- <http://slp.icheme.org/hazops.html>
- http://www.acusafe.com/Hazard_Analysis/Hazard_Analysis-HAZOP.htm
- <http://www.ipk.ntnu.no/fag/SIO3020/Overheads/hazop6.pdf>
- NSW Department of Urban Affairs and Planning, 1995. *Hazard and Operability Studies*, Hazardous Industries Planning Advisory Paper No 8. ISBN 0 7310 3080 X. This useful resource is only available as a hardcopy. The publication can be purchased online (<http://www.planning.nsw.gov.au>) or alternatively contact the Department to order the publication.

Fault Tree Analysis

- http://reliability.sandia.gov/Reliability/Fault_Tree_Analysis/fault_tree_analysis.html
- <http://www.sverdrup.com/safety/fta.pdf>
- <http://web2.concordia.ca/Quality/tools/15fta.pdf>

Event Tree Analysis

- <http://www.sverdrup.com/safety/eventtree.pdf>

Failure Modes, Effects and Criticality Analysis (FMECA)

- <http://www.relexsoftware.com/reliability/fmea.asp>
- http://www.acusafe.com/Hazard_Analysis/Hazard_Analysis-fmea.htm

Human Error Analysis (HEA)

- http://www.ida.liu.se/~eriho/WhatIsHRA_M.htm
- http://www.ida.liu.se/~eriho/Publications_O.htm

Click on "Downloads" and select the following documents:

- Hollnagel, E., Pedersen, O. M. & Rasmussen, J. (1981) (7.6 MB)
Notes on Human Performance Analysis
- Hollnagel, E. (1983) (78 KB)
Position paper for NATO Conference on Human Error
N J Bahr "System Safety Engineering and Risk Assessment: A Practical Approach" Section 8.2 Human Factors Analysis Publisher Taylor and Francis ISBN 1-56032-416-3

Level of Protection Analysis (LOPA)

- Centre for Chemical Process Safety (CCPS), 2001. *Layer of Protection Analysis: Simplified Process Risk Assessment*, Pub No: G-66, American Institute of Chemical Engineers AIChE, New York, NY. ISBN No: 0-8169-0811-7. The publication can be purchased online (<http://www.aiche.org/pubcat/seadtl.asp?ACT=S&Title=ON&srchText=layer+of+p+rotection+analysis>) or alternatively contact the AIChE Customer Service to order the publication.
- A. M. Dowell and D. C. Hendshot, Rohm and Haas Company, 2002. *Simplified Risk Analysis- Layer of protection Analysis (LOPA)*, National Meeting Paper 281a. American Institute of Chemical Engineers AIChE.
- E. M. Marszal and E. W. Scharpf, *Systematic Safety Integrity Level Selection (with Layer of Protection Analysis)*, ISA Publications. This reference is only available as a hardcopy. The publication can be purchased online (<http://www.isa.org/Template.cfm?Section=Books&Template=/Ecommerce/ProductDisplay.cfm&ProductID=4517>).



The quality of Risk Assessment deliverables is greatly influenced by selecting the right method to review the system or issue identified by the Objective. THIS IS A KEY ISSUE.

4.1.5 Selecting Risk Analysis Method – the Means of Calculating and Examining the Level of Risk

Risk Analysis is about developing an understanding of risk. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost effective strategies. Risk analysis involves consideration of the sources of risk, their positive and negative consequences and the likelihood that these consequences may occur. HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004. As such, Risk Analysis involves different ways of calculating risk considering “how often” (probability or likelihood) and consequences (or severity).

Like the previous requirement to match the Risk Assessment method to the Objective / Expected Deliverable, it is important to match the Risk Analysis method to the Objective / Expected Deliverable.

4.1.5.1. Risk analysis methods

There are 3 types of risk analysis methods, qualitative, quantitative and semi-quantitative.

4.1.5.1.a. Qualitative risk analysis

Qualitative analysis uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. These scales can be adapted or adjusted to suit the circumstances and different descriptions may be used for different risks. HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004.

Qualitative risk analysis methods are used to set priority for various purposes including further analysis. They are useful when reliable data for more quantitative approaches is not available.

Some techniques are as basic as the one below, suitable for categorising risk based on individual or team opinion.

Table 4.10 Example of a basic qualitative risk analysis matrix

	High Likelihood	Medium Likelihood	Low Likelihood
High Consequence	HIGH		MEDIUM
Medium Consequence		MEDIUM	LOW
Low Consequence	MEDIUM	LOW	LOW

There is no description of the difference between high, medium or low, simply the words. Therefore it remains for the person(s) who use this method to decide of those differences. As such, it is a very rough method of risk analysis that simply divides the identified risks into 3 categories – red, green and yellow.

It is not likely that any risk assessment method, other than Informal Risk Awareness for Day-to-Day Tasks would use this approach.

Here is another example. This has been adapted from a version used in a number of industries. The reference given later in the section provides information on a wide range of such matrices used in different circumstances.

Table 4.11 Example of Risk Definition and Classification

Likelihood Ranking Table

*Likelihood	Description	#Frequency Description	
		Safety Example	Health Example
Almost Certain	Consequence is expected to occur in most circumstances	High frequency of occurrence-occurs more than once per year	1 case per 100 person years
Likely	Consequence will probably occur in most circumstances	Event does occur, has a history, occurs once every 1-10 years	1 case per 1000 person years
Possible	Consequence should occur at some time	Occurs once every 10-100 years	1 case per 10,000 person years
Unlikely	Consequence could occur at some time	Occurs once every 100-1000 years	1 case per 100,000 person years
Rare	Consequence may	Occurs once every 1000-	1 case per 1,000,000

	occur under exceptional circumstances	10000 years	person years
--	---------------------------------------	-------------	--------------

*Likelihood of impact occurring eg fatality, hearing loss etc.

#The frequency descriptions must be generated for each specific risk assessment so that the timeline is appropriate to the level of detail of the risk assessment

Consequence Severity Ranking Table

		Company Levels (3-7)					Critical
		Low	Minor	Moderate	Major		
Business Levels (2-6)		Low	Minor	Moderate	Major	Critical	
Site Level (1-5)		Low	Minor	Moderate	Major	Critical	
Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Level 7	
Injury and Disease							
No medical treatment Low level short term subjective inconvenience or symptoms. No measurable physical effects	Objective but reversible disability impairment and /or medical treatment injuries requiring hospitalisation	Moderate irreversible disability or impairment to one or more persons	Single fatality and/or severe irreversible disability or impairment to one or more persons	Short or long term health effects leading to multiple fatalities or significant irreversible human health effects to >50 persons	Short or long health effects leading to >50 fatalities or very serious irreversible health effects to >500 persons	Short or long term health effects leading to >500 fatalities or very severe irreversible human health effects to >5000 persons	
Cost							
\$10,000	\$10,000-\$100,00	\$100,000-\$1M	\$1M-\$10M	>\$10M	>\$100M	>\$1000M	

In this example the consequence levels are identified differently for different parts of the organisation. The site uses levels 1 – 5, the business levels 2 – 6 and the company levels 3-7. The consequences are those appropriate for consideration at the defined levels.

The measures in this table should reflect the needs and nature of the organisation and activity under consideration to determine the level of concern.

Consequence (or Severity) is the worst outcome that could realistically result from the unwanted event.

When using any method to estimate risk there is often an important question. Should the likelihood or probability be estimated considering existing controls or without controls in place. There is no absolute answer to this question. The above scale, as with any other similar matrix, can be used for either approach. However, it is important for the Scope to identify which approach will be taken in the exercise. It is recommended that if controls exist and are credible, the assessment should consider them.

In particular, it would be sensible to include consideration of existing controls when estimating Likelihood or Probability when the system being examined has a significant operating history. In this case the team would find it unrealistic to consider the risk without the existing controls that have been in place for some time.

See Section 3.6 on Risk Assessment Pitfalls

If the risk assessment is being Scoped to review a new project or system, the team must decide and record the decision whether or not the risk is to be looked at with or without the new or planned controls.

The important point is to establish whether or not existing controls will be considered while estimating Likelihood or Probability in the Scoping stage of the risk assessment.

Once the Probability and Severity numbers are selected, a comparative risk can be identified from the Table below:

Table 4.12 Risk Ranking Table

Likelihood or Frequency	Consequence Severity				
	Low	Minor	Moderate	Major	Critical
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Possible	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Note: The number of categories should reflect the needs of the study

Legend:

Letter	Risk Level	Risk Control Measures
E	Extreme Risk	<ul style="list-style-type: none"> ▪ Immediate action required, activity must not start or if started must be stopped. ▪ Identify and implement controls to reduce risk to Low before starting or recommencing the activity ▪ Highest level corporate management needs to be involved.
H	High Risk	<ul style="list-style-type: none"> ▪ Immediate action required, activity must not start or if started be must stopped. ▪ Identify and implement controls to reduce risk to Low before starting or recommencing activity. ▪ Senior site management needs to be involved.
M	Moderate Risk	<ul style="list-style-type: none"> ▪ Complete risk assessment ▪ Identify hazards and implement controls to reduce risks ▪ Management responsibility must be defined.
L	Low Risk	<ul style="list-style-type: none"> ▪ Identify hazards and implement controls as required ▪ Manage by routine processes

The two selections are combined in a table to provide Risk Ranks. Sometimes each cell in the table is ranked in order.

A second well known example of such a Risk Ranking process is that developed by the US Military and NASA.

Table 4.13 NASA/US MIL SPEC 882D Risk Ranking Method

Probability Estimate

Identifier	Descriptor
A	Common event or likely to occur (>.1)*
B	Probably will occur or "it has happened" (0.1 – 0.01)
C	May occur or "heard of it happening" (0.01 – 0.001)
D	Not likely to occur or "never heard of it" (0.001 – 0.000001)
E	Practically impossible (<.000001)

*unwanted event expected to happen 1 in 10 times the circumstances occur

Maximum Reasonable Severity Class (People)

Identifier	Descriptor
I	Catastrophic – fatality or permanent disability
II	Critical serious lost time injury/illness
III	Moderate – average lost time injury/illness
IV	Minor lost time injury/illness

The two selections are combined in a table to provide Risk Ranks. Sometimes each cell in the table is ranked in order, sometimes cells are categorised as suggested in the NASA/US Military Specification example Table 4.13

Table 4.14 Risk Ranking Table

	Probability A	Probability B	Probability C	Probability D	Probability E
Severity I	1	1	2	3	4
Severity II	1	2	3	4	5
Severity III	2	3	4	5	6
Severity IV	3	4	5	6	7

There are many variations on design of qualitative analysis approaches. However, the description or numerical ranges must be carefully defined to meet Objectives as well as provide discreet and suitable choices.

For example, to explore more information on various Qualitative Risk Analysis approaches try

- <http://www.planning.nsw.gov.au/plansforaction/mihaps-docs/mihaps-docs.html>
Appendix 2 of MIHAP No 3 Hazard Identification, Risk Assessment and Risk Control. This reference provides a comparison of 10 models including AS/NZS (1999)
- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN14_MHFR.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN14_MHFR.pdf)

4.1.5.1.b. Quantitative risk analysis

Quantitative Risk Analysis involves the calculation of probability, and sometimes consequences, using numerical data where the numbers are not rank (1st, 2nd, 3rd) but rather “real numbers” (i.e. 1, 2, 3, 4 where 2 is twice 1 and half of 4).

As such, accurate quantification of risk offers the opportunity to be more objective and analytical than the qualitative or semi-qualitative approaches.

Most commonly, quantification of risk involves generating a number that represents the probability of a selected outcome, such as a fatality. Following is an example of probabilistic information concerning the risk of a fatality per year. British Nuclear Industry research suggests the following probability of death from various causes in the UK. The figures are based on past history.

Lightning	-	.0000001	or	1 in 10 million
Fire / explosion at home	-	.000001	or	1 in 1 million
Death in a 'safe' industry	-	.00001	or	1 in 100,000
Death in a road traffic accident	-	.0001	or	1 in 10,000
Death in mining	-	.001	or	1 in 1,000
Flying in commercial aircraft ¹	-	.00001	or	1 in 100,000
Smoking	-	.05	or	1 in 200

The history of fatalities in the Australian mining industry from 1991 to 2001 suggests the following⁶.

Risk of death in Australian mining	-	.0005	or	1 in 5,000
------------------------------------	---	-------	----	------------

Most Quantitative Risk Analysis for industrial applications attempts to establish probabilities of unwanted events and subsequently the probability of the consequences from the unwanted event. For example, the risk of a total large petroleum storage tank structural failure might be .003 per year. If there are multiple events that must happen before a major loss can occur then assigning numerical probabilities allows for risk calculations that are normally not possible with qualitative or semi-qualitative data.

Fault Tree

This may be done by using the rules from Fault Tree Analysis to construct a Fault Tree. The example in Figure 1.2 below shows a fault tree listing all the components potentially involved in the failure of an emergency lighting system. The construction starts at the “top event”, in this case the “no light from emergency lighting system” and proceeds level by level until all fault events have been traced to their basic contributing causes.

This may require working through several levels or it may be satisfied in one. In the

⁶ Based on Data from Minerals Council of Australia surveys

example the tree has stopped at defective wiring , which is possibly sufficient, but there may be circumstances, determined by the boundaries placed, where this needs to be explored to the next level of “incorrect wiring” or “wires chewed by rats” or ”wiring cut by sharp edge in conduit” etc

The fault tree, when analysed, allows all the combinations of events that can lead to the top event to be identified .

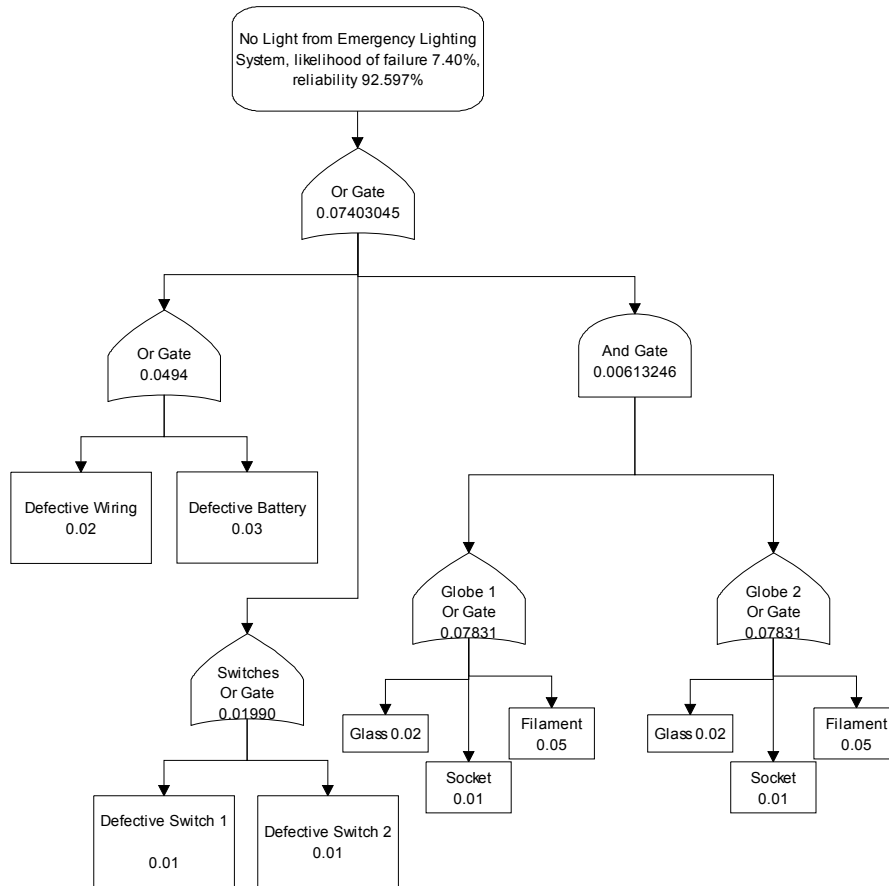


Figure 4.15 An example of quantitative risk analysis using a fault tree

The example illustrates the use of a modelling method to identify contributing factors to an unwanted event. Fault Tree Analysis is one of several methods that can be used to model an unwanted event. In the example numbers in each initiating event (the rectangles) represents the probability that the initiating event will occur. The “And Gate” and “Or Gate” shapes indicate the relationship of the initiating events below to the events above the gates. An “Or gate” indicates that the event above will occur if any of the initiating events below occur. Therefore the probability of the event above is based on adding together all the probabilities in the initiating event rectangles. The “And Gate” indicates that all initiating events below must occur to create the event above. In this case, the initiating event probabilities are multiplied. It must be noted that to analyse the fault tree to obtain the combinations of events that result in the top event (minimal cut sets) (the process of solving the fault tree) involves the use of Boolean Algebra for all

manipulations of the fault tree. It is recommended, that for other than the simplest fault tree, a specialist is consulted for this activity.

Assuming the probabilities are reasonably accurate, a quantitative risk analysis based on a systematic event model can yield a reasonably realistic probability of the major unwanted event (the initiating event or the top event in a Fault Tree). Most importantly, FTA maps out all of the contributing factors in a potential incident scenario, which in turn allows the most critical initiating events to be identified and hence identifies the best area for implementing further controls. In addition, the FTA allows new probabilities to be entered into the tree and a new top event calculation to be made, thus providing a demonstration of the effectiveness of the intended controls and allowing a cost benefit analysis to be done (bearing in mind however the possible requirement of ALARP, SFAP, ALAP etc).

Event Tree

A similar modelling method can be used to extend the analysis from the probability of the major unwanted event to identify the probability of different outcomes or consequences. This is known as an event tree. In the case of a fault tree, the process is started from the unwanted event and works from the so called top event down. An event tree starts with a particular unwanted event and works from the bottom up.

The first example, Figure 4.16, illustrates the probability of the consequences from an unwanted event defined as "Release of Flammable Gas". In the example the release of a large cloud of flammable gas is the unwanted event, this may be from an LPG storage tank on site struck by a truck and the tank or pipeline punctured. A number of issues need to be considered, the cloud may ignite at once, or after a delay or not at all. With immediate ignition ie as soon as the escape starts, the result will almost certainly be a fire. With delayed ignition, the result may be a flash fire or an explosion. The probability of fatality of a particular person will depend on whether the incident is a fire, a flash fire or an explosion. In this example the leak is determined to occur 1 in 10 years and there are probabilities assumed for immediate ignition, delayed ignition etc. The outcome, using the dummy data, is a very high risk of fatality of 0.0299pa (requiring immediate action, if the data was correct, by the addition of appropriate barriers to reduce the probabilities).

The second example, Figure 4.17, is constructed in the same fashion but using equipment failure rates per demand. The example is that of the power supply to a mine operation from a power station failing. This has been determined from the fault tree as happening 1 in 10 years despite all the control measures in the system. There is a back up diesel on site which is supposed to switch in on power failure and, if that fails, there is a battery back up for critical applications. The outcome is an indication of just how secure or insecure the power supply system is in the event of principal supply failure. The top/unwanted event is "Principal Power Supply Fails". The outcome is the frequency of emergency power failure. The outcome calculated of 0.000255 failures per year is probably acceptably low. An ongoing check would be needed to test the performance of the diesel and the battery system to ensure their performance was not deteriorating because of lack of maintenance etc.

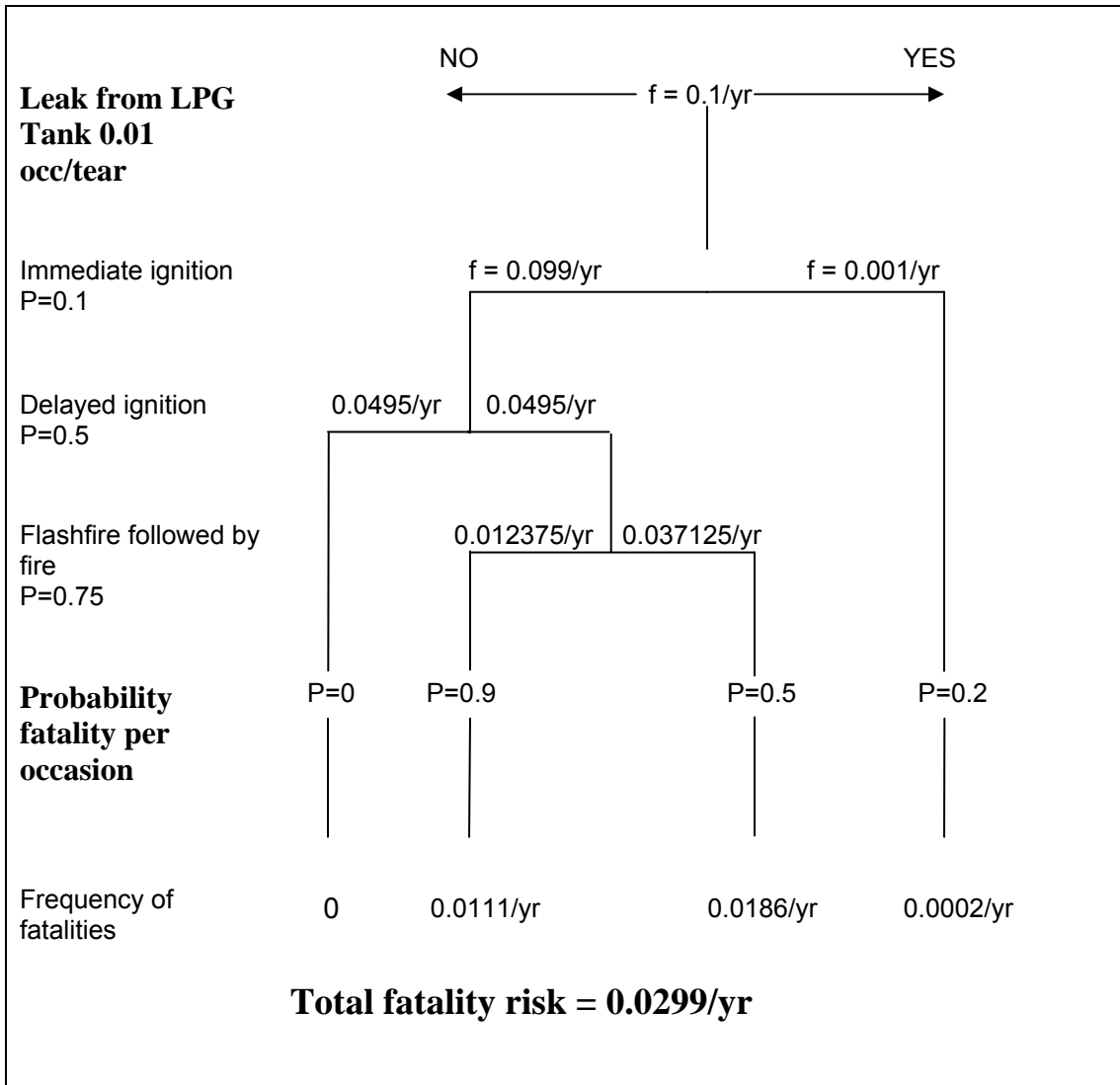


Figure 4.16 Event Tree (Gas Release)⁷

⁷ Adapted from ICI Engineering Hazan Course Notes

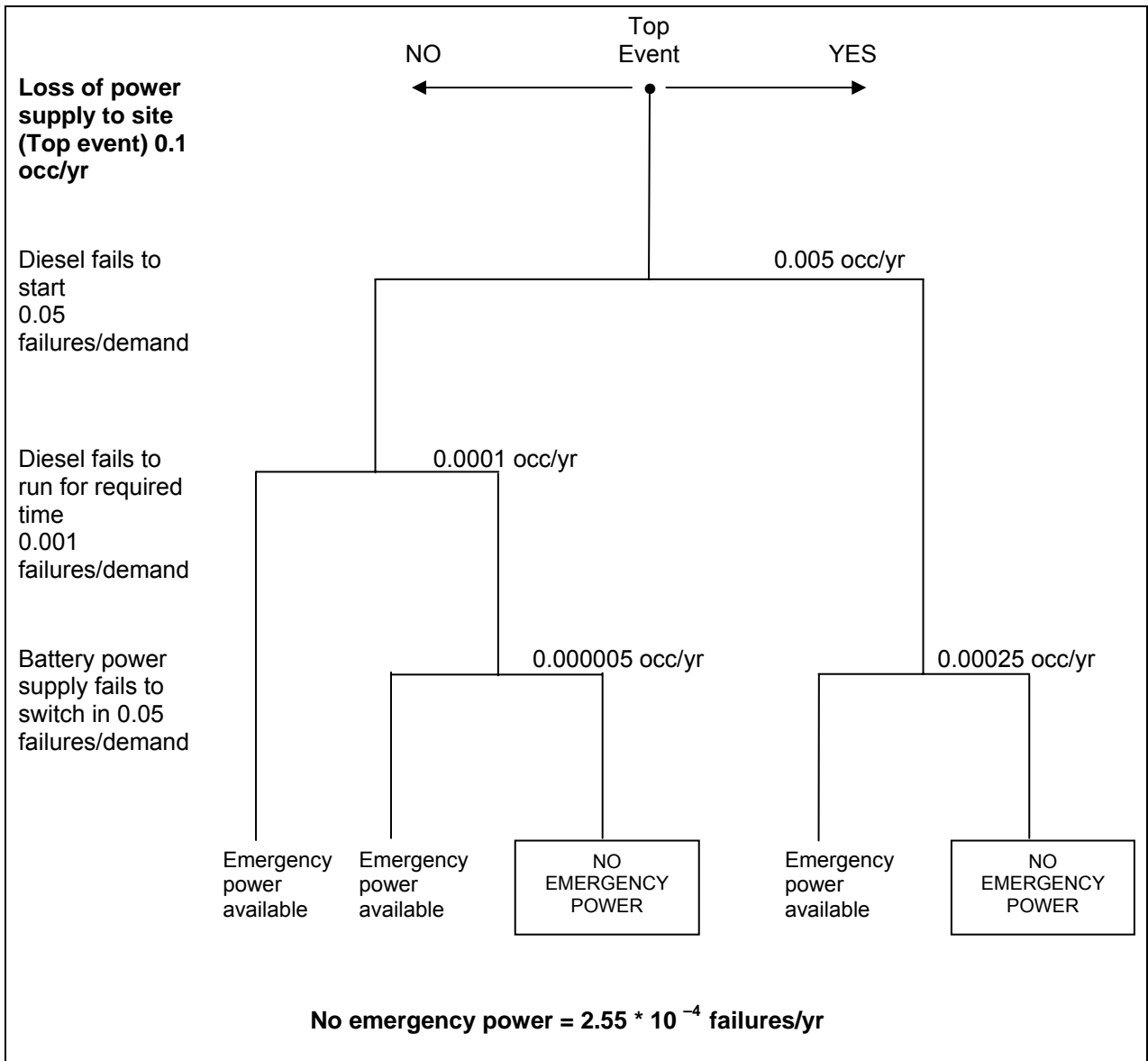


Figure 4.17 Event Tree (Power Supply) ⁸

Level of Protection Analysis (LOPA)

This analysis form is a relatively new development and is still developing, the references noted earlier should be consulted for more detail. It has been effectively used in some safety cases as a means of demonstrating adequacy of protection LOPA is a variation of event tree analysis where only two outcomes were considered and has found a particular use in working with Safety Instrumented Systems (SIS) but not exclusively. The possible outcomes are either “unwanted impact” or “no event”. Each analysis starts at the unwanted event frequency that starts the event tree. Beyond the initiating event

⁸ Adapted from Lees Loss Prevention in the Process Industries

there are a number of event tree branches, each of which represents a layer of protection. Each branch has only two paths, one for propagation of the event and the other for "no event" Each layer of protection has to be independent of the unwanted event and other layers of protection, these are referred to as IPLs (independent protection layers). If they are not truly independent the resultant risk estimate will be too low. The analysis is, in some usages described as semi quantitative as it does use numbers to calculate a numerical risk, however the numbers used are conservative and rather than closely represent an actual performance of specific systems provide order of magnitude results. Figure 4.18 shows the principal of the approach.

IPLs need to meet certain tests of function to qualify, apart from independence. They need to detect or sense a condition in the scenario, make a decision on action and deflect the undesired consequence. It is noted that procedures and inspections cannot be treated as protection as they do not meet the tests.

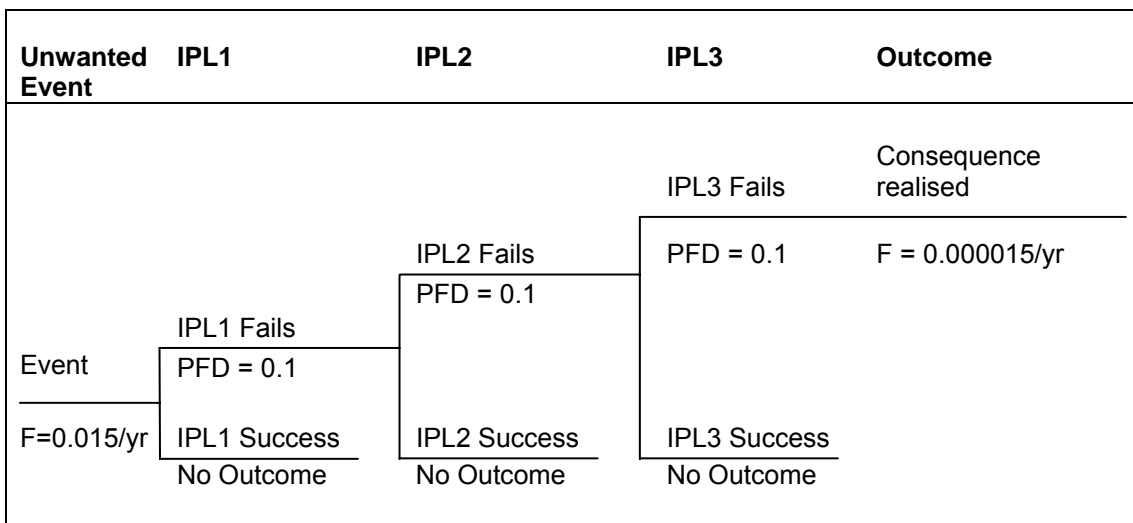


Figure 4.18 LOPA Principles Example

A helpful presentation of the overall picture of an unwanted event is shown in Figure 4.19. This is called a Bow Tie Diagram⁹. The unwanted event is given in the centre of the Bow Tie. On the left hand side is given the causes and hazards that potentially lead to the event. Also shown are the controls or barriers to the event occurring, these are the proactive controls and are typically classified as Elimination (of the Hazard) or Prevention (of the event). The right hand side of the diagram is the event tree which shows the various outcomes that potentially can occur and the controls or barriers that are in place for after an event occurs are also shown. These are the Reactive Controls and are typically classified as Reduction (of the consequence) or Mitigation (of the consequence). Clearly the preference is for successful proactive control but reactive control is also essential to minimise harm after an event. See section 4.1.1.D for more discussion on control measures.

For further information on the Bow Tie Diagram try the following references

⁹ Adapted from ICI Plc Hazan Course Notes 1979

[http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN14_MHFR.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN14_MHFR.pdf)

<http://www.absconsulting.com/resources/THESIS/FABIG-Issues37.pdf>

<http://quintec.com/esas03/papers/ESAS03-TheUseOfBowTieAnalysisinOMESafetyCases.pdf>

<http://www.eagle.org/news/pubs/surveyor/dec99/ism.htm>

http://www.porttechnology.org/journals/ed11/downloads/pt11_189-192.pdf

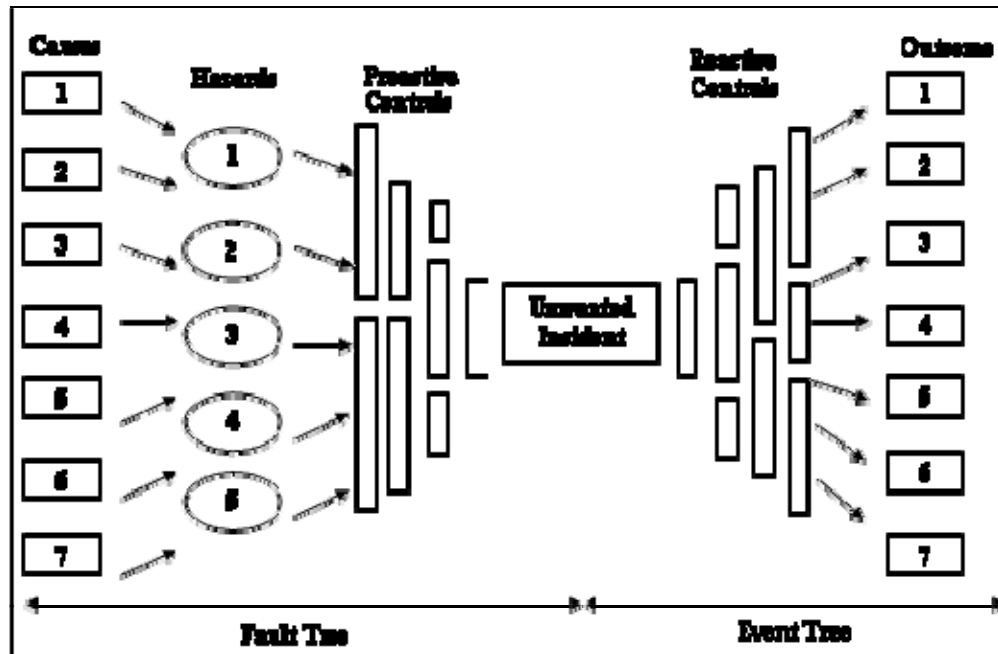


Figure 4.19 “Bow Tie” Diagram

Should the risk assessment require quantitative consideration of different events, consequences can be quantified by establishing a common unit for all of the potential losses, such as dollars. Depending on the circumstances, this may require establishing the value of a human life.

The accuracy of probabilistic data is sometimes challenged, especially when the numbers are multiplied, potentially exacerbating any inaccuracies. Obviously the accuracy of the data is determined by the validity of the source. It is uncommon for a minerals company or organisation to have extensive probabilistic data especially where human activity is concerned. There are several commercial services that supply probabilistic data on hardware failures and some sources of human reliability data.

For example, to explore more information on various probabilistic data approaches try:

- http://www.mishc.uq.edu.au/publications/Databases_for_Equipment_Failure011.pdf

For example, to explore more information on various risk analysis approaches try:

- http://home1.pacific.net.sg/~thk/quant_r.html - (re: Human Error)

- http://www.mishc.uq.edu.au/publications/Risk_Analysis_Methods_a_Brief_Review.pdf
- <http://www.jbfa.com/gratechniques.html>
- <http://www.sti.nasa.gov/new/prass14.html#TOP>
- <http://www.yellowbook-rail.org.uk/site/resources/models/yellowbookR1.pdf>
- <http://www.hq.nasa.gov/office/codeq/doctree/ftbh.pdf>
- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN14_MHFR.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN14_MHFR.pdf)
- Centre for Chemical Process Safety, 1992. *Guidelines for Hazard Evaluation Procedures*.

For example to explore more information on various control measures approaches try:

- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN10.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN10.pdf)

LESSONS LEARNED 4.6

There is some history of attempts to assign quantitative probabilities to events without valid source information. When this happens it is probable that the assigned probability is no more accurate than semi-quantitative methods. The problem may arise when assumptions are made about the accuracy of the probability or a risk that has been calculated if this is then to be used as part of a decision making process.

4.1.5.1.c. Semi Quantitative Risk Assessment

The content of this section was supplied by QEST Consulting of Melbourne¹⁰ and describes the technique that they have developed for SQRA. This technique has been used extensively and successfully in the Mining and Minerals Industry although originally developed to meet the needs of the Safety Case in Victoria.

There are currently two spectral extremes in risk assessment methodologies:

- Quantitative Risk Assessment (QRA)
- Qualitative Risk Assessment

These are discussed in detail in sections 4.1.5.1.a Qualitative Risk Assessment and 4.1.5.1.b Quantitative Risk Assessment.

The approach In Quantitative Risk Assessment, although exhaustive and detailed, is clearly not foolproof and has two primary shortcomings. One is the misleading output

¹⁰ QEST Consulting <http://www.qest.com.au>

when the selection of failure statistics is not well considered. The second is the fact that much of the decision making in the assessment of risk is inevitably done by a consultant.

The result of a Qualitative Risk Assessment is usually high team member buy-in as they made all of the decisions. However, the accuracy and transparency of the process is extremely poor because of the crudity of the measures used, as is its value in prioritising risk reduction actions.

The SQRA approach is something of a mixture of the two extremes.

QUEST SQRA attempts to match the thoroughness of QRA in identifying all of the failure modes but then asks a series of “bite sized” questions of a representative site/engineering team to establish the risk value. In so doing, workforce buy-in is maintained but identical units of measurement of risk such as Potential Loss of Life (PLL) can be generated based on the team’s decisions. The process is less costly than QRA but the balance of the primary objectives is often considered to be substantially better than either of the other options (quantitative or qualitative). It must be recognised that the SQRA process probably provides greater accuracy in regard to the *relativity* of the risks than it does in regard to *absolute* values. Nevertheless, the risk values (PLL) generated are a reasonable basis for rationalising risk reduction measures.

The steps in the SQRA methodology are as follows (using a workshop/team based approach).

1. Whilst viewing the left-hand side of the bow-tie diagram (see *), assess the frequency of **the initiating event**. The example shows an initiating event estimated to occur once in 100 years.

Occurrences per Year		10+	6-9	3-5	2	1	No Fatality
1+	One or more						
0.1	Less than 10						
.01	< 100						
.001	< 1000						
.0001	< 10,000						
.00001	< 100,000						
.000001	< 1000,000						

2. Whilst viewing the both sides of the diagram, assess the number of time there

.01	< 100								980
-----	-------	--	--	--	--	--	--	--	-----

3. Distribute the remaining occurrences across the section of outcomes (eg. 1 fatality, 2 fatalities, 3-5 fatalities etc.)

.01	< 100	1	1	2	4	12	980
-----	-------	---	---	---	---	----	-----

- Calculate PLL values (fatalities per annum) by multiplying likelihood by the sum of the consequences.

$$i. 01*((1*11.5)+(1*7)+(2*4)+(4*2)+(12*1))/1000 = 0.000385 \text{ or } 3.85*10^{-4}$$

- A sample risk profile as initially assessed (SQRA Base Case) follows. This assessment assumed the mine to be operating with existing controls in their existing condition.

Table 4.10 SQRA Base Case

SQRA for Precious Gold Mine

Row #	Hazard	Frequency Risk Rating	Sample Size	1a	1b	2a	2b	3	4	5	Max Fatal	Risk 10 ⁻⁶	Risk
1	PCW UC 181	0.78	0.000					20	20	0.000	0.0000	0.00E+00	0.00%
2	PCW UC 182	4	0.000					0	0	0.000	0.0000	4.00E+00	0.00%
3	PCW UC 183	7	0.000					0	0	0.000	0.0000	7.00E+00	0.00%
4	PCW UC 184	3	0.000					0	0	0.000	0.0000	3.00E+00	0.00%
5	PCW UC 185	0.7	0.000					0	0	0.000	0.0000	0.70E+00	0.00%
6	PCW UC 186	4	0.000					0	0	0.000	0.0000	4.00E+00	0.00%
7	PCW UC 187	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
8	PCW UC 188	2.8	0.000					0	0	0.000	0.0000	2.80E+00	0.00%
9	PCW UC 189	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
10	PCW UC 190	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
11	PCW UC 191	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
12	PCW UC 192	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
13	PCW UC 193	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
14	PCW UC 194	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
15	PCW UC 195	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
16	PCW UC 196	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
17	PCW UC 197	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
18	PCW UC 198	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
19	PCW UC 199	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
20	PCW UC 200	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
21	PCW UC 201	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
22	PCW UC 202	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
23	PCW UC 203	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
24	PCW UC 204	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
25	PCW UC 205	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
26	PCW UC 206	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
27	PCW UC 207	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
28	PCW UC 208	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
29	PCW UC 209	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
30	PCW UC 210	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
31	PCW UC 211	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
32	PCW UC 212	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
33	PCW UC 213	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
34	PCW UC 214	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
35	PCW UC 215	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
36	PCW UC 216	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
37	PCW UC 217	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
38	PCW UC 218	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
39	PCW UC 219	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%
40	PCW UC 220	0.8	0.000					0	0	0.000	0.0000	0.80E+00	0.00%

There is no generally accepted maximum level of risk at which a facility should operate and regulators continue to avoid specifying criteria for demonstrating maximum risk levels. Clearly, any actions to improve the critical controls associated with these hazards are amongst those at the top of the actions priority list. See discussion on Risk Acceptability in Section 4.1.5.B. and footnote in Section 4.1.1.A on ALARP, SFAP etc.

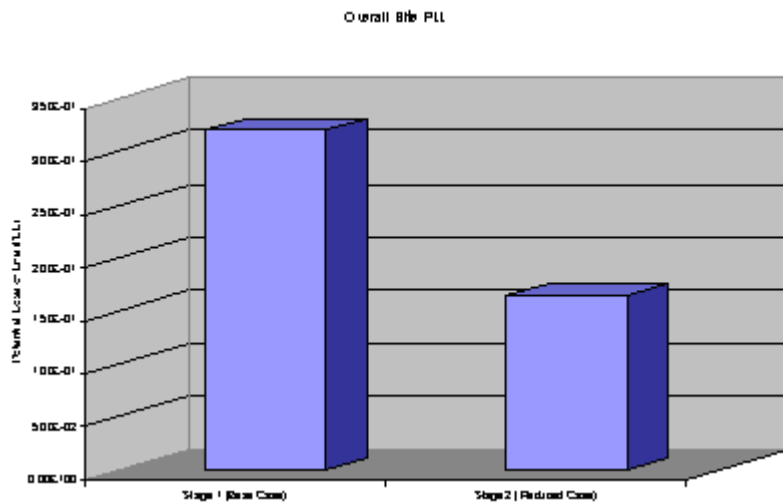
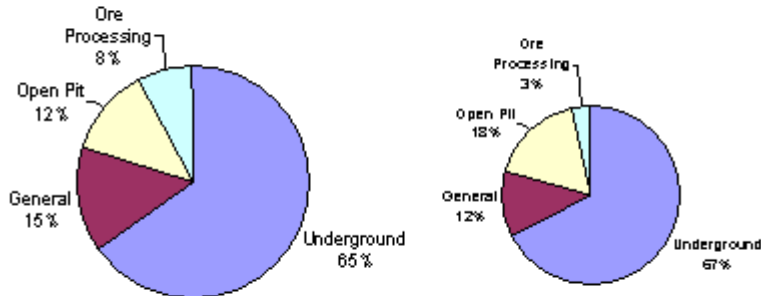


Figure 4.7 SQRA Comparisons of Base and Reduced Cases

Precious Gold SQRA Results

Overall Risk Reduction = 48%



Base Case PLL = 0.321
(Fatalities per Annum)

Reduced Case PLL = 0.166
(Fatalities per Annum)

Also clear from the examining the base case and reduced case tables is the fact that major risk reduction on relatively few hazards has brought about most of the improvement.

The site profile after implementation of the actions is as shown below.

Whilst it should be remembered that all of the risk values are more accurate in regard to relative risk than absolute risk, three conclusions can be safely assumed:

- The safety assessment process has heightened awareness of the critical risk areas and provided a framework within which to identify and address the priority issues.
- The 'safety case' approach and the adoption of the SQRA process has been 'repeatedly successful in showing the way to further safety risk level reductions.
- When the critical actions are completed, the approach can be used to identify ongoing risk reduction as part of a continuous improvement program.
- Because the risks were assessed using SQRA, the business is in a position to maintain the entire safety process in-house if desired.

Whilst the SQRA may be the engine room of a risk assessment, as with the best of QRAs, the overall process asks and derives answers for all of the following questions:

- If it can, how often can it occur given the existing controls?
- How bad will the consequences be if it does occur?
- What are the most critical of our controls?
- How effective are they (dependable, understood, practical, monitored)?
- What should we do to improve things within practicable limits?
- In what order should these things be carried out?
- If all our controls failed, could this be expected on occasions to result in a fatality?

Table 4.11 SQRA Reduced Case

SQRA Reduced Case for Precious Gold Mine

Rank	Hazard No.	Hazard Title	Frequency Originating Event	Sample Size	10+	100	1000	2	1	Non- Fatal	Risk 10 ⁶	Risk	%Risk
1	POW UG001	Rock falls during ground support installation	3	1000	0	0	0	1	9	990	30000	3.00E-02	19.99%
2	POW UG005	Personnel, Vehicles or Equipment in Proximity to Walls - Falling In	0.125	1000	0	0	0	20	980	900	27900	2.79E-02	16.64%
3	POW UG002	Rock falls during charging development faces	2	1000	0	0	0	1	4	995	12000	1.20E-02	7.28%
4	POW UG006	Personnel/Vehicles/Equipment Close to Walls - Working Below	1	1000	0	0	0	2	8	990	12000	1.20E-02	7.28%
5	POW UG010	Unauthorized access / criminal activity incidents	25	10000	0	0	0	1	1	998	7500	7.50E-03	4.72%
6	POW UG011	Contact with overhead or underground electrical services	0.5	1000	0	0	1	2	7	990	7500	7.50E-03	4.54%
7	POW UG015	Heavy Vehicle/Light Vehicle/Person Interaction - Underground	1	1000	0	0	0	1	4	995	6000	6.00E-03	3.63%
8	POW UG008	Vehicle or equipment rollovers	0.05	1000	0	0	1	9	90	900	9900	9.90E-03	3.33%
9	POW UG012	Shovel Hoisting Equipment	0.002	1000	10	80	100	100	80	900	5400	5.40E-03	3.31%
10	POW UG001	Heavy Vehicle - Light Vehicle Collision	0.033	1000	0	0	5	20	100	975	5280	5.28E-03	3.15%
11	POW UG005	Falling from edges (personnel, light vehicle, heavy vehicle)	0.033	1000	0	0	0	0	100	900	3900	3.90E-03	2.00%
12	POW UG018	Unplanned Detonation of Explosives during Operations	1	1000	0	0	0	0	3	997	3000	3.00E-03	1.81%
13	POW UG003	Rock fall from in-belt beams and rollers striking personnel	0.01	1000	0	0	0	25	225	750	2700	2.70E-03	1.69%
14	POW UG002	R/Wall Failure	0.01	1000	0	15	15	20	50	900	2525	2.52E-03	1.59%
15	POW UG004	Dropped Object in Road/Shaft	1	1000	0	0	0	0	2	998	2000	2.00E-03	1.21%
16	POW UG011	Vehicle /personnel Interactions	0.01	1000	0	0	0	0	200	900	2000	2.00E-03	1.21%
17	POW UG014	Uncontrolled Mobile Plant Fire	0.02	1000	1	1	4	10	34	990	1700	1.70E-03	1.05%
18	POW UG012	Vehicle Impact with Stationary Object	0.05	1000	0	0	0	5	25	970	1700	1.70E-03	1.05%
19	POW UG017	Contact Loss or Remotely Operated Mobile Equipment	0.03	1000	0	0	0	0	5	995	1650	1.65E-03	1.00%
20	POW UG003	Rock falls during uphole production charging	0.25	1000	0	0	0	1	4	995	1500	1.50E-03	0.91%
21	POW UG002	Material Falls from Conveyors and Structures	15	10000	0	0	0	0	1	999	1500	1.50E-03	0.91%
22	POW UG005	Personnel Falling from Elevated Work Platforms	0.005	1000	0	0	0	0	300	700	1500	1.50E-03	0.91%
23	POW UG005	High Pressure Pneumatic/Hydraulic Systems	0.5	1000	0	0	0	1	1	998	1500	1.50E-03	0.91%
24	POW UG019	Large Fall of Ground	0.1	1000	0	0	1	2	7	990	1500	1.50E-03	0.91%
25	POW UG007	Vehicle, equipment or material released from ROM subgrade or wall	0.003	1000	0	0	0	0	100	900	1000	1.00E-03	0.75%
26	POW UG010	Transport of ore to peak site by public road - vehicle accident	0.00007	1000	1	2	7	40	50	900	12302	1.23E-03	0.74%
27	POW UG003	Light Vehicle Travel on Public Roads (Company Vehicles)	4	10000	0	0	0	1	1	998	1200	1.20E-03	0.73%
28	POW UG008	Mud or Water Rush	0.00007	1000	1	2	7	20	70	900	10922	1.09E-03	0.69%
29	POW UG005	Personnel Falling into Openings (Floor Grating, Tanks, Bins)	0.02	1000	0	0	0	0	50	950	1000	1.00E-03	0.60%
30	POW UG005	Concentration of Gases	0.25	1000	0	0	0	1	2	997	1000	1.00E-03	0.60%
31	POW UG005	Material or personnel falling from equipment or plant during maintenance	0.04	1000	0	0	0	0	25	975	1000	1.00E-03	0.60%
32	POW UG004	Material falls from excavator or truck in production cycle striking person	0.004	1000	0	0	0	0	200	800	800	8.00E-04	0.45%

4.1.5.2. Risk acceptability

This is no zero risk situation. All actions, decisions or situations involve some level of risk, though in most cases the risk is very low. Very low or reasonable risk is considered to be acceptable. Many regulatory frameworks require the management of risk to a level that is reasonable but fall short of defining the specific criteria for major unwanted events such as an occupational fatality.

In many risk assessments it may be necessary to determining the level of acceptable risk during the Scoping process.

Many environmental regulatory agencies require that risk to the public from activities on a proposed new industrial site be less than 1 in one million fatalities per year. Social research has indicated that the community considers acceptable occupational fatality risk to be 1 in one hundred thousand, or ten times higher than public risk. However, the later figure is not currently specified in any mining related regulations.

Information in the previous section of this Guideline suggested that the overall risk of fatality in the Australian minerals industry is approximately 1 in five thousand, based on 1991 to 2001 data. This indicates that, as an industry, we are performed significantly higher than the 1 in one hundred thousand figure.

The diagram below is commonly used to explain the concept of acceptability and ALARA. ALARA is an acronym for “as low as reasonably achievable”.

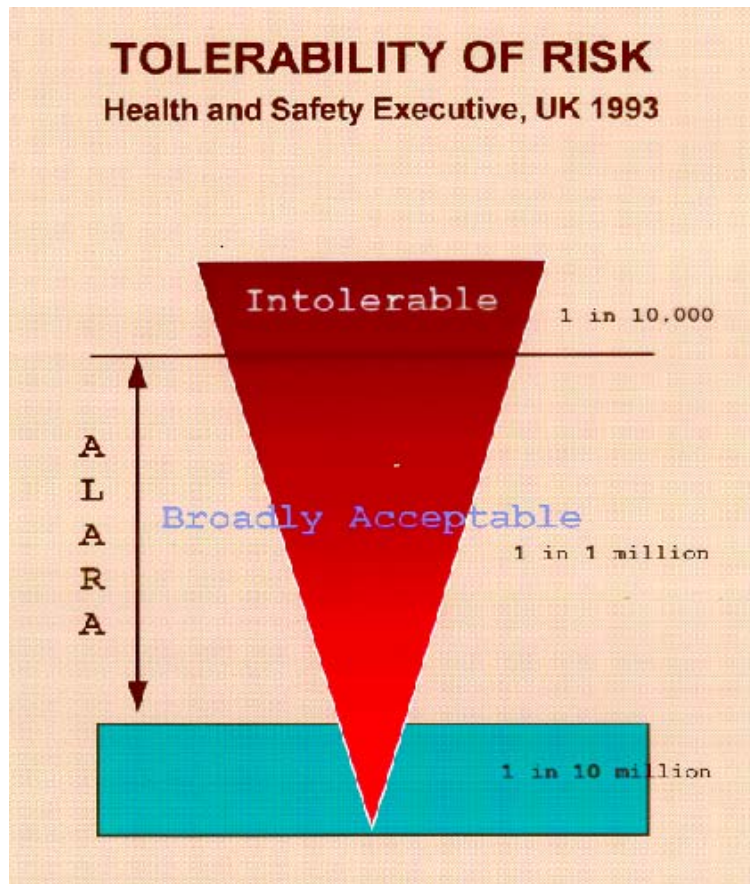


Figure 4.8 Risk tolerability, ALARA

Risk acceptability, for the purpose of a minerals industry risk assessment will be important to establish in the Scoping stage. However, the precision of the risk acceptability criteria may vary with the Objective.

If the Objective of the risk assessment does not involve specifically determining acceptability, the intent may be to identify the priorities for risk reduction. In this later case, the use of an accepted qualitative or semi-quantitative risk analysis technique may be adequate. In this case, the risk analysis technique may supply a cut off classification where risk is seen to be “low”.

If the Objective of the risk assessment requires determination of acceptability, then quantitative techniques would likely be most appropriate. In this case it would be desirable to establish an acceptable probability of the unwanted event or if there are varied unwanted consequences, an acceptable risk level incorporating objective consequence units such as dollars.

Despite the above discussion, it must be borne in mind that it is possible under some regulatory regimes that the expectation will be that of SFAP or some similar expression. This term may be defined in legislation or regulation and it would be prudent to determine what local legislation prescribes. SFAP in Victoria means all risks must be

reduced so far as practicable. Although the test of practicability includes consideration of the risk level, which means that measures that would be implemented if the risks were high would not necessarily be implemented if the risks are low, this never eliminates the need to identify and implement all practicable risk reduction measures. In the same legislation is also the requirement for continuous improvement which must be allowed for in any attempt to identify acceptability.

For example to explore more information on various risk acceptability approaches try:

- [http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN16.pdf](http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN16.pdf)
- Department of Urban Affairs and Planning NSW; Hazardous Industry Advisory Paper 4, Risk Criteria for Land Use Planning
- DNV Technica; Risk Assessment Guidelines; Prepared for ACC and the Victorian Government, Project no A1196. {Available from Health and Safety Organisation, Vic}, Melbourne 1995, (Chapter 6).

4.1.5.3. Selecting the method considering the expected deliverable

The following table suggests the different example Risk Analysis methods that might be considered for each desired deliverable. Note that any or all of the noted options might be used depending on the Objective.

The example risk analysis methods mentioned in the table are:

Qualitative Risk Analysis (Qual RA)- To very roughly discuss and group risks

Semi – Quantitative Risk Analysis (SQRA) - To identify rough priorities for the profile, often where exposure is a key factor to focus on priorities, further study and analysis

Semi Quantitative Control Code Analysis (CRC) See section 4.1.5.1.4 for discussion - To judge the appropriateness of controls for the identified risk but note that ranks should not be compared

Quantitative Risk Analysis (QRA) - To more accurately establish the probability of unwanted events to mathematically manipulate and/or consider acceptability

Risk / Benefit Analysis (RBA)- To identify the most cost effective controls for an unacceptable risk

Table 4.12 Possible Applications of various Risk Analysis Methods for Potential Objectives / Expected Deliverables

Potential Deliverable / Objective	Qual. RA	SQRA	CRCA	QRA	RBA
Formal Safety Assessment Development	X	X	X	X	X
Risk Profile or Register Development	X	X			
Risk Acceptability Determination		X	X	X	X
Information for Major or Principal Hazard Plans	X	X	X	X	X
Information for Operational Guidelines	X	X	X		X
Information for Maintenance Plans or Guidelines	X	X	X	X	X

Hardware / Processing Design Reviews	X	X	X	X	X
Option Review	X	X	X	X	X
Review of Change Management Plan	X	X	X		X
Information for drafting of SOPs	X	X	X		
Informal Risk Awareness / on Day-to-Day Tasks	X				

As the table illustrates, the selection of the appropriate risk analysis technique is primarily related to the degree of precision that is required and the quality of available data.

4.1.5.4. Re-analysis of risk considering new controls

The Re-ranking of risk considering a no control to control situation or an existing to new control situation is becoming a more common practice in the minerals industry.

LESSONS LEARNED 4.7

Many mining operations are using semi-quantitative risk ranking techniques to re-rank unwanted event scenarios after they are initially ranked without adequate controls. This practice is fraught with potential error. Semi-quantitative scales were not designed for this type of analysis. A drop of 1 level of probability roughly equates to a magnitude change (or 10 times less likely to occur). A drop in 1 level of consequence equates to an entirely different level of potential energy release, achievable only through redesign of the system to reduce the amount of energy in the system.

The degree to which a control reduces the probability and/or consequence of an unwanted event varies depending on the type of control and the way it is applied. The System Safety Society in the United States has published the following method for rating controls. It is intended for use in conjunction with the NASA / Mil Spec 882B example Risk rank table (Table 4.14) outlined earlier in section 4.1.5.1.a.

Control Rating Code (CRC) Method

Control Effectiveness = Type of Control X Control Strategy

1. Identify each control intended to reduce one of the ranked risks
2. Assign the type of control, based on the I to V Hierarchy of control types.
3. Assign the control strategy or the objective of the type of control, based on the A to E strategies.

Table 4.13 Hierarchy of Control Type

Hierarchy of Control Type		
I	- Design Change	- a hardware feature that is intended to fully control the energy
II	- Passive Safety Device	- a device not requiring action to operate as a control
III	- Active Safety Device	- a device requiring action to operate as a control
IV	- Warning Device	- a device that warns of an unwanted energy condition
V	- Procedure	- a procedure intended to control

Table 4.14 Energy Control Strategy

Energy Control Strategy	
A - Eliminate Energy Source	- control objective is to totally eliminate the energy so no longer exists in the system (i.e. no consequence)
B - Limit Energy Accumulated	- control objective involves reduction of the available energy (less consequence)
C - Prevent Energy Release	- control objective is to control energy so it should not be released
D - Provide Barriers to Energy Flows	- control objective is to protect, once the energy is released
E - Change Release Patterns	- control objective is to protect, once the energy is released
F - Treat / Minimise Harm	- control objective is to protect / reduce damage on or at the person

Once the Hierarchy of Control and the Energy Control values are selected, a single Control Rating can be selected from the Table below:

Table 4.15 Control Rating Code Table

Energy Control Strategy I V	I Design Change	II Passive Safety Device	III Active Safety Device	IV Warning Device	V Procedure
A Eliminate Energy Source	1	1	2	3	3
B Limit Energy Accumulated	1	1	2	3	3
C Prevent Energy Release	1	2	2	3	3
D Provide Barriers to Energy Flows	2	2	3	4	4
E Change Release Patterns	2	3	4	4	5
F Treat / Minimise Harm	3	3	4	5	5

As an indicator of risk acceptability, Residual Risk, is often considered acceptable if the Uncontrolled Risk Rank (from the previous qualitative NASA / Mil Spec Table 4.13) is equal to or less than the Control Rating Code (Risk Rank – Control Rating = 0 or greater). Sometimes a situation where the Control Rating is 1 higher than Risk Rank can be considered acceptable but not ideal. If the Control Rate Code is 2 or more ranks higher than the Risk Rank it is most unlikely that the risk would be considered acceptable – other options must be discussed.

LESSONS LEARNED 4.8

Some sites rank risks considering existing controls when they identify probability and consequence (which is fine). However, a control only affects probability or consequence - not both. Most controls reduce probability of an event (but never to zero). Only controls that reduce or eliminate the source energy being controlled actually reduce consequences, which means different incident event scenarios will need to be considered. Note that isolation or de-energising does take away the energy but if the lock, tag or procedure fails, the energy release is still the originally available energy amount – therefore consequence is not reduced.

4.1.5.5. Risk / Cost benefit analysis

Risk/Cost Benefit Analysis may also be part of a Risk Assessment Objective. Risk/Cost Benefit Analysis is often used as one criteria to help select the most effective control options to address an unacceptable risk. Techniques in this vary. Some examples are given below for consideration.

Potential Loss of Life/Implied Cost of Averting Fatality

The Potential Loss of Life (PLL) is the number of fatalities that can be expected to occur each year, averaged over a long period. It is a measure of societal risk. The number should be small: if 100 people are each exposed to a risk level of 10 in a million per year, the PLL is 0.001.

The PLL is a useful basis for cost benefit analyses of risk reduction measures, via the “Implied Cost of a Fatality” (ICAF):

$$\text{ICAF} = \text{cost of measure} / (\text{initial PLL} - \text{reduced PLL})$$

Such calculations are often controversial as they appear to require a value to be placed on human life, but these calculations are commonly used internationally, and may be suitable to aid decision making in regard to adopting control measures for major hazards. For example, a low ICAF for a proposed risk reduction measure implies that it is highly effective, because the cost is low compared to the risk reduction achieved. Conversely, a high ICAF implies a relatively ineffective risk reduction measure, indicating that perhaps the money should be diverted to an alternate. It is however, as stated earlier, only one of the criteria to be used.

The following table gives some guidance to using the cost to avoid a fatality in decision making:

Cost to Avert One Fatality In \$A	Assessment
1,000	Highly effective; always implement
10,000	
100,000	Effective; always implement
1,000,000	Effective; implement unless risk is negligible
10,000,000	Consider, effective if individual risk are high
100,000,000	Consider at high risk levels or if there are other benefits
1,000,000,000	Ineffective

Cost Benefit

One measure of risk is the cost the operator would face if the hazard were to be realised. If the consequences of the hazard can be meaningfully expressed in economic terms, then cost benefit analysis can be used to help set priorities and aid decision making.

The cost of implementing the solution or control measure can usually be determined readily, as money will usually need to be expended. Both the capital cost and ongoing operating costs will need to be taken into account. The cost can then be annualised using, for example the remaining plant life.

The benefit from the solution is actually the reduction of the cost of the hazard and can be determined by computing the annual cost before and after. This will require some quantitative risk assessment work, although in simple cases estimates can give at least an indication.

For example, consider a hazard that might occur once in 100 years and cost \$10million in total damages. Assume that a control exists that will reduce this to once in 500 years at a cost of only \$1 million. Assume that the control costs \$500,000 IN Capital, \$10,000pa in operating cost, and will last ten years, so the annual cost is \$60,000. The benefit is:

$$B= H1-H2$$

$$= (\$10,000,000/100 \text{ years}) - (\$1,000,000/500 \text{ years}) + \$98,000 \text{ pa}$$

Hence the cost benefit ratio is 60,000/98,000 = approx 0.6. The lower the cost benefit ratio, the more attractive the expenditure.

Note that while this method is attractive to ensures, it does not take into account the cost of potential human suffering and should not be used as a primary decision criterion for safety and health related hazards. Similarly a cost benefit ratio greater than 1 is not a valid reason not to implement a safety related improvement. The cost benefit ration can at best be used as another tool to help rank priorities amongst a range of actions.

A similar tool introduces the concept of the Potential Control Effectiveness into the equation, again a tool only.

The Cost of the Problem per year (CP/yr) must be greater than the Cost of the New Control per year (CNC/yr) considering the Potential Control Effectiveness (PCE). PCE is never 100%.

$$CP/yr > CNC/yr * PCE\% \text{ (expressed as decimal, i.e. } 70\% = .70)$$

None of the above takes into account the requirement that is imposed in may regimes requiring the ALRP principal be applied. Cost benefit is not necessarily a factor.

For example to explore more information on Risk/Cost Benefit Analysis approaches try:

- <http://www.sjsu.edu/faculty/watkins/cba.htm>
- [http://www.workcover.vic.gov/vwa/home.nsf/pages/so_majhaz_guidance/\\$File/GN16.pdf](http://www.workcover.vic.gov/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN16.pdf)

LESSONS LEARNED 4.9

When reviewing procedures that are existing or new controls, it is common for risk assessment teams to over-estimate their effectiveness at reducing risk, especially when considering procedural controls for extreme or high risk situations. Generally, procedural controls rely on human reliability and therefore are considered to be moderately effective controls at best. It would be most unlikely that a procedural control could conceivably reduce a risk effectively by one order of magnitude, which is the equivalent of moving a risk one place on a risk assessment matrix. It should also be noted that for major or catastrophic risks, the use of a procedure as a control would not be considered credible unless there were other substantial control measures further up the hierarchy covering the risk. See Section 5.7 on the Hierarchy of Controls.

4.1.6 Range of External Influences to be Considered

This covers any outside influences that are not within the study boundaries but which may have implications within the study boundaries or be influenced by the process being studied.

Some of the issues that may be covered by this are:

- Cyclones
- Indigenous communities
- Fly in fly out rosters
- Government requirements
- Earthquake

4.1.7 Consequences of Interest

These may be the site/facility generic consequences of interest or they may be tailored for specific needs to include lower (never higher) consequences as the threshold for identifying controls.

Some of the consequences that may be considered by this are:

- Permanent damage
- Plant availability
- Environmental discharge in excess of compliance limits

4.1.8 Core Assumptions

The core assumptions are features of the area or process to be studied which can reasonably be assumed during the study.

Some examples of the core assumptions that may be made in this section might be:

- The equipment is/is not fit for its intended use
- The operators are/are not trained adequately
- The Company policies are/are not enforced
- The process or equipment will/will not work as designed
- Accurate SOPs were/were not available to those who needed them

4.1.9 Selecting a facilitator for the risk assessment

When applying risk assessment methods that involve the use of a team, a process facilitator should be considered to achieve the following goals:

- Establish clarity about direction, roles and the risk assessment process
- Establish an appropriate method for making group decisions
- Provide expertise on the appropriate study methodology and in successfully leading study teams
- Provide an assessment of the adequacy of the information supplied for the assessment
- Recognise when a more appropriate technique should be used for part of the assessment

- Communicate at all levels
- Work through unresolved conflicts that cause barriers to the process and work towards consensus
- Provide the organisation for the team process
- Improve the way of identifying hazards, assessing risks and discussing controls

All significant risk assessments should have a facilitator. As the complexity of the risk assessment increases the required skill level of the facilitator will also increase.

LESSONS LEARNED 4.10

There are many examples of past risk assessments where the lack of appropriate facilitator skills has led to an inadequate and ineffective risk assessment exercise.

4.1.10 Determining the composition of the team or working groups

Risk assessment teams or working groups should comprise a relevant cross-section of personnel with varying perspectives on the system in order to provide a broad depth of experience and background to the risk assessment. Obtaining an appropriate balance between the following disciplines should be considered in team member selection:

- Management personnel with a system overview
- Technical and supervisory personnel from technical services, maintenance or production areas related to the system
- Trades and operational personnel from maintenance, production or processing plant areas
- An expert or experts in the area that is the subject of the risk assessment
- A facilitator (appropriately competent in the selected Risk Assessment method)
- A recorder or scribe, this should not be the facilitator but could be one of the team members who has the appropriate skills of accurate minute talking etc

A team of between four to eight persons would be typical of a risk assessment exercise. More may be required for specialist input but the team must be kept as small as practical so that it is able to operate as a team. "Observers" are to be discouraged.

4.1.11 Deciding the time required (and venue)

The schedule and length of time for any team exercise should be specified in the scoping document as should the venue and any special requirements associated with the venue.

4.1.12 Risk assessment result and feedback

The method and process for ensuring that the risk assessment has the desired output should also be specified in the scoping document. The Scope might include information on the following areas.

- Expected output (formal report, action plan, input into work order system, meeting presentation, etc.)
- Accountability for required action, including converting information output into desired overall deliverable (Formal Safety Assessment, Plan, SOP, etc.)
- Method of communicating action to be taken back to the risk assessment team or working group
- Method and timing of follow up to ensure required actions were undertaken

Following the preceding steps carefully should result in an effective Scope for a quality Risk Assessment.

Finally and very importantly, to have an adequate Scope for a risk assessment there should be a document that outlines at least these 12 areas:

- 1. An objective based on the expected deliverable**
- 2. A description of the system to be reviewed including the physical and/or process boundaries**
- 3. An inventory of the potential hazards**
- 4. The Risk Assessment method – the means of identifying the potential unwanted events**
- 5. The Risk Analysis method – the means of calculating and examining the level of risk**
- 6. A statement of the external influences that are to be considered as a minimum**
- 7. Clear identification of consequences of interest in the study context**
- 8. A listing of core assumptions**
- 9. The Facilitator for the Risk Assessment**
- 10. The Risk Assessment team or work group**
- 11. The time required (and venue)**
- 12. The means of providing risk assessment results and the desired Deliverable with accountabilities and timelines**

5. Doing the Risk Assessment

Most risk assessment projects will require some form of facilitated team exercise. Some risk assessments, or parts thereof, may involve work by individuals outside the team. For example, individuals may gather information on the system, hazards, probabilities or other areas that will be considered in the overall assessment.

Since the vast majority of projects involve team exercises this Section will focus on the quality of that approach and, specifically, the process of facilitating a team exercise.

The process of facilitating a Risk Assessment requires several important ingredients.

- A clear, accurate Scope for the Risk Assessment (see the previous Section)
- Appropriate resources (team, data, time, etc. as defined in the Scope)
- A facilitator with appropriate knowledge and skills for the exercise

A facilitator is a person whose role in a risk assessment is to drive the risk assessment process, as outlined in this Section of the Guideline. He/she leads the team through a specific risk assessment method, focussing on the quality of the process. The facilitator does not provide technical input on the system, hazards, risks or controls. That is the role of the team.

The facilitator may challenge or question the team by suggesting risk management principals or concepts in the process. For example, the team may not discuss a relevant type of hazard or underestimate the consequences of an event. In this type of situation the facilitator must suggest to the team that they revisit or rethink the issue.

Facilitation is a skill and, as such, the more complex the risk assessment the more important the skill.

For example, to explore more information on various Facilitation Skills approaches try:

- <http://www.socialimpact.com/TNFacSkl.html>

The facilitator is often directly involved in preparing the Scope with the client for the risk assessment. As previously outlined, this is a very important step.

Once the Team exercise has been scheduled, it remains for the facilitator to lead the session. An agenda for the session may include, depending on the specific risk assessment method, the following items.

- Introducing the scope to the team
- Reviewing the system
- Identifying the hazards
- Identifying the potential unwanted events
- Analysing the risks
- Evaluating the acceptability of the risks
- Considering existing controls or barriers

- Identifying new controls or barriers
- Closing the Exercise

Note that the information in many steps must be recorded as part of the process and for subsequent report requirements. The method of recording can vary and should be selected based on method requirements. Report format is addressed in the next section of this guideline.

5.1 Introducing the scope to the team

The Scope document should outline the design and rationale for the risk assessment project. As such it can be used to introduce the team to the task. The facilitator can extract relevant information from the Scope document such as that related to the 8 areas mentioned in the previous section, or at least:

- Objective (including eventual required deliverable)
- System boundaries
- External influences
- Consequences of interest
- Core assumptions
- Hazard types or Issues to be addressed
- The Risk Identification and Risk Analysis methods
- Time requirements
- Expected output and subsequent action process

This information should be presented to the team before the exercise commences.

5.2 Reviewing the selected system

The next step should involve a discussion about the system, project or topic being reviewed by the risk assessment process. The purpose of this step is to ensure that all team members have an adequate understanding of the system and the boundaries of the system before starting to identify hazards.

Depending on the Risk Identification tool and the exercise complexity this step may involve one or more of the following:

- Developing and discussing a process map of the system being reviewed (i.e. for a PHA/WRAC, FTA or more detailed assessment)
- Reviewing an existing process map of the system,
- Reviewing a Process and Instrumentation Diagram (P&ID) (i.e. for a HAZOP)
- Reviewing a component illustration of the hardware (i.e. for a FMECA),
- Reviewing the operations or design of new equipment with an Original Equipment Manufacturers (OEM) representative.

The facilitator must ensure that the team understands the system, as well as the relevant system boundaries as defined in the Scope, being examined well enough to input into the risk assessment process.

5.3 Identifying the hazards

As previously mentioned, the quality of a risk assessment greatly depends on the recognition that:

- Firstly – identify and understand the hazards
- Secondly – identify the unwanted events and assess the specific risks

The Scope may provide a Hazard Inventory Table to the team. This table would outline the hazard types and clarify any uncertainties about any specific hazard (see Section 4.1.3 “**Identifying and understanding the potential hazards**”). If available the facilitator should review the table to ensure that the team understand the type, nature and magnitude of the hazards that are to be considered when the system is reviewed.

If the Hazard Inventory Table is not supplied in the Scope, the facilitator should lead the team in a discussion identifying the types of hazards, their nature and magnitude. If any hazard is unclear that uncertainty must either be clarified or the facilitator must define the uncertainty and gather information from the team to document the assumptions made about the hazard. **THIS IS A KEY ISSUE**. Failure to clarify assumptions about the nature or magnitude of a hazard can lead to inadequate controls and the assumption of unacceptable risk.



In some cases it may be necessary to do Consequence Analysis before a Risk Assessment exercise so that the team is clear on the potential outcomes of an event.

The facilitator should ensure that the team members understand the types of hazards being considered in the exercise before proceeding.

5.4 Identifying the potential unwanted events

The Risk Identification method, as well as the relevant system boundaries for review, should have been specified in the Scope. The example team-based methods discussed in this Guideline include the following:

- Job Safety / Hazard Analysis (JSA / JHA)
- Energy Barrier Analysis (EBA)
- Preliminary Hazard Analysis / Workplace Risk Assessment and Control (PHA / WRAC)
- Hazard and Operability Study (HAZOP/CHAZOP)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Level Of Protection Analysis (LOPA)

- Failure Modes, Effects and Criticality Analysis (FMECA)
- Human Error Analysis (HEA)
- SIS

Each example method is intended to address different desired deliverables and each method varies in the way it prompts the identification of unwanted events. The following table illustrates the differences in the various methods. Note that it is only a basic illustration to show typical differences. More detailed information can be found at the relevant web sites identified earlier.

Table 5.1 Illustrating the Different Approaches to Identifying Unwanted Events in Various Example Risk Identification Tools

Risk Identification Method	Approach to looking for Unwanted Events
Job Safety / Hazard Analysis (JSA / JHA)	Walk through the task reviewing each of the current task steps and, considering the hazards, identify specific unwanted events
Energy Barrier Analysis (EBA)	Follow the energy flow from event initiation through to maximum reasonable consequence, identify relevant existing barriers or controls between each energy step and identify barrier failure events
Preliminary Hazard Analysis / Workplace Risk Assessment and Control (PHA / WRAC)	Walk through the process map reviewing each box and, considering the hazards, identify specific unwanted events
Hazard and Operability Study (HAZOP)	Walk through the P&ID, node by node, and considering the hazards, identify specific unwanted events
Fault Tree Analysis (FTA)	Using a defined unwanted terminal event, deduce from general potential contributors to more specific contributors, the unwanted events that could possibly lead to that event
Event Tree Analysis (ETA)	Using a defined unwanted initiating event, deduce the subsequent events that could occur as the event escalates to various outcomes, identifying the unwanted events that could possibly lead to a major terminal event
Level of Protection Analysis (LOPA)	Using simplifying rules, LOPA starts with an identified unwanted incident scenario frequency and evaluates independent Level of Protection and consequences to provide an order of magnitude estimate of risk. It is a version of an event tree analysis.
Failure Modes, Effects and Criticality Analysis (FMECA)	Walk through the component illustration, component by component, and considering the failure modes of that component, identify significant unwanted events
Human Error Analysis (HEA)	Walk through the process map of the relevant task, action by action, and considering the error types, identify specific unwanted events

Once the facilitator is confident that the system has been reviewed within the defined boundaries or, in the case of FTA and ETA, the illustration has been completed the exercise can proceed to establishing the risk of each unwanted event.

5.5 Analysing the risk

Sometimes analysing risk is not part of the exercise. For example, Job Safety or Hazard Analysis, and HAZOP, do not usually involve formal Risk Analysis. In JSA and HAZOP, unwanted events are identified and then controls or barriers are discussed. If this applies the facilitator should skip the next two sections.

In most cases some form of Risk Analysis is applied, whether it be qualitative, semi-quantitative or quantitative. The Facilitator and the team should know the method of analysing risk before starting this step from the Introduction at the beginning of the exercise.

The selection of the Risk Analysis method should have been part of the Scoping process (see Section 4.1.5 “**Selecting the risk analysis method – the means of calculating and examining the level of risk**”).

It is important with some methods to identify whether the Risk Analysis is done considering existing controls or barriers. For example, is the likelihood and consequences of an electrical contact while using a hand tool to be estimated considering that there is a current well established, procedure to inspect the tool before use, or should the risk be estimated considering the event without the procedure?

Like many areas of Risk Management there is no set answer to this question. It is determined by the design or Scope of the project, considering the Objective and the degree to which the team will be comfortable with the method.

However, the following basic examples may help clarify the issue:

- If the Objective involves reviewing a new system where controls are not in place – consider likelihood and consequence **without** controls
- If the Objective involves reviewing an existing system where robust controls are in place – the likelihood and consequence should always be considered **with** existing controls

The Facilitators role in this step is as follows:

- Ensure that all team members understand the risk analysis method, including any guidelines for acceptability
- Apply the risk analysis method to each unwanted event accurately. (Note that analysing risk considering existing controls may require the facilitator to use the Control Rating Code method or, at least, its principals) **THIS IS A KEY ISSUE.**
- Monitor for bias, over-confidence or inaccuracy in the application of the method and, if relevant, challenge the team. Does it make sense? **THIS IS A KEY ISSUE.**

The facilitator should ensure that all identified unwanted events have been assigned a level of risk.

5.6 Evaluating the risk acceptability

The selected Risk Analysis method for the team exercise may indicate risk acceptability levels as part of design. Often Risk Analysis methods are included corporate procedures for Risk Management or Risk Assessment. Therefore, the facilitator should know the relevant risk acceptability criteria before the exercise and, subsequently, ensure that the team understands the information.

In qualitative and semi-quantitative Risk Analysis methods the intent usually involves ordering the unwanted events by level of risk. Acceptability criteria may be illustrated in the method by a “green” or specific low risk rank level. In this case the acceptability criteria simply identify the lowest priority risks. Normally, qualitative and semi-qualitative methods are not used to determine acceptability but rather to focus discussion on higher priority risks. There are, of course, exceptions for some specific methods such as in Control Rating Code method, applied to increase the accuracy of the Risk Analysis.

If a quantitative technique has been applied, there may be defined acceptability criteria such as a probability. For example, the figure, .00001 fatalities per year (as discussed in Section 4.1.5.2), is considered to be an acceptable fatality rate for workplace risks.

The facilitator will often lead the discussion on acceptability as part of the previous risk analysis step. Whatever the case, the facilitator must try to ensure that no unwanted event, with or without controls, is unacceptably deemed to be an acceptable risk therefore not requiring improved controls. **THIS IS A KEY ISSUE.**



5.7 Considering existing controls or barriers


Existing controls may have been identified before or after the Risk Analysis method was applied, as previously discussed.

Independent of the timing or the specific Risk Identification tool, the facilitator should help the team identify existing controls. To prompt the teams' generation of existing controls that facilitator might use the Hierarchy of Controls list. Note that effectiveness decreases from top to bottom of the list.

- **Elimination** – remove the hazard so consequence is virtually zero
- **Substitution** – replace or reduce the magnitude of the hazard so there is less consequence (note that replacing introduces a different hazard)
- **Isolation** – remove the hazard or the target at the time of exposure
- **Engineering Controls** – reduce the probability of the unwanted event through hardware design
- **Administrative Controls** – reduce the probability of the unwanted event through procedural approaches
- **Personal Protective Equipment** – reduce consequences at the target

It is sometimes easiest for the facilitator to start the discussion of controls by referring to the highest risk event and proceeding down the list to the lowest risk or the predefined acceptability criteria. This focuses the teams' energy on the highest risks and also controls for higher risks often affect moderate risk events too.

Deciding whether controls are adequate for the risk level can often be subjective even when attempting to apply quantitative risk analysis techniques.

 To determine whether controls are adequate the facilitator should consider the following options. **THIS IS A KEY ISSUE.**

- **Use the Rule-of-Two** – at least two engineering or more effective controls per unwanted event should be in place for an extreme or high risk.
- **Use the Control Rating Code** – use the CRC to discuss or formally analyse control effectiveness
- **Use a quantitative approach** - calculate control reliability as part of event probability

The facilitator should ensure that all existing controls for unacceptable risks are considered.

5.8 Identifying new controls or barriers

If an unacceptable risk remains after existing controls are considered, the facilitator should lead the team through a discussion of possible new controls or barriers to reduce the risk further.

Again the Hierarchy of Control and the 3 adequacy considerations listed above should be considered.

This guideline offers a brief overview of Risk/Cost Benefit Analysis. Risk / Cost Benefit Analysis can be used to select the best controls from suggested options. It may or may not be part of the Scope.

Minimally, the facilitator should ensure that all unacceptable risks are addressed with existing or new controls until the residual risk is considered to be acceptable.

5.9 Closing the risk assessment

The final step in the exercise requires the facilitator to close the exercise by checking that the Scope has been fulfilled, expressing appreciation for the contribution of the team, and communicating the expected future actions from the Scope to the team.

Note that the facilitator may also be responsible for documentation of the Risk Assessment exercise.

5.10 Summary of the Risk Management Process for Common Situations

In this section a summary is provided of the possible application of the risk management process for a range of situations that commonly occur in the life of a mining operation ie existing operations, changes to existing operations, new mine projects and acquisitions and divestments.

What is the process?

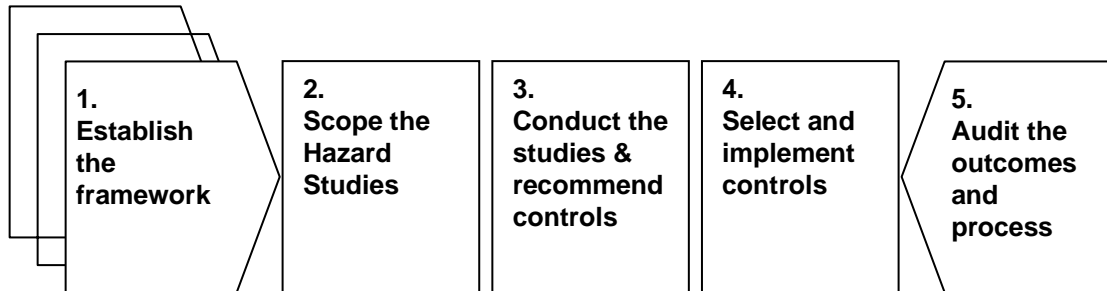


Figure 5.1: Hazard management process steps

Hazard management can be considered as a five step process:

- **Step one varies according to whether you are working on an existing mine operation, changes in those existing operations, or a new mine project**
- **Steps two to four are a generic Risk Assessment Process**
- **Step five captures the need to review all aspects of hazard management to improve future processes and outcomes**

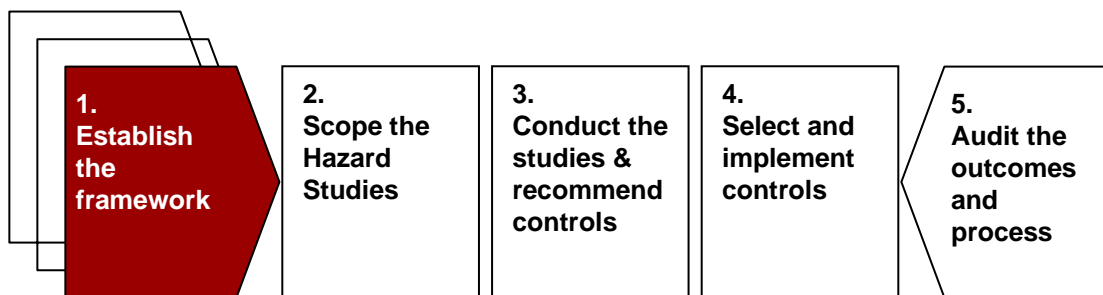
Each element is expanded further in the following pages. The primary intent of the process is to ensure that appropriate systems are in place to:

- Identify hazards to people, plant and environment
- Assess the risk posed by those hazards
- Manage those hazards that are determined to be an unacceptable risk by eliminating the hazard, reducing the risk or controlling hazard as far as practicable.

It is important that any unit can demonstrate to all the stakeholders in the mine, including the statutory authorities, that these systems are in place and operating effectively. In some cases, rigorous legislation may require units to take a different approach with more detail required than suggested here.

TABLE 5.2 – STEP 1 ESTABLISH THE FRAMEWORK

	Existing Operations	Changes to Existing Mine Operations	New Mine Projects	Acquisitions & Divestments
Standard	Hazards on existing mine sites should be systematically identified and appropriate controls established. The mine plan and design must be subject to regular review MAKE IT SAFE	All changes to a mine plan or design should be assessed for impact and controls established prior to implementation KEEP IT SAFE	All mine projects should be planned, designed and implemented to maximise inherent safety and reduce risk. Major changes should be treated as new mine projects. BUILD IT SAFE	All acquisitions and divestments should be assessed to determine safety, health and environmental risks. TRADE IT SAFE
Requirements	<p>You should:</p> <ul style="list-style-type: none"> Conduct a high level mine review to identify the need for and priority of further detailed risk assessments Revisit the hazard Register and update as required. Plan the time and resources required to complete the identified risk assessments. Some high-risk hazards may require detailed expert study, while others may be of low enough risk that they need no further study at all. Conduct the risk assessments consistent with the quality required by this Guideline Schedule and implement the actions arising from the risk assessments in a timely manner Regularly (6 monthly) audit the hazard evaluation and implementation processes Periodically (5 yearly) revalidate the risk assessments 	<p>You should:</p> <ul style="list-style-type: none"> Identify and register changes to plan, design, plant, people, the environment and systems. Changes are potential ways to introduce new hazards. Filter changes to determine those which: <ul style="list-style-type: none"> Can be approved without risk assessments Require risk assessments prior to approval Cannot be approved Conduct the risk assessments consistent with the quality required by the company policies Implement the actions arising from the risk assessments prior to making the change Regularly (6 monthly) audit the change management processes Ensure the hazard register is updated each time 	<p>You should:</p> <ul style="list-style-type: none"> Develop a Hazard Inventory Conduct risk assessments at each major stage of a new mine project, consistent with the generic stage process. Determine the type and extent of risk assessments appropriate for the stage At each stage, review risk assessments from the previous stage (if applicable) Conduct the risk assessments consistent with the quality required. Schedule and implement the actions arising from the risk assessments in a timely manner Regularly audit the risk assessment program and progress throughout the project. Include special projects, such as decommissioning, demolition, rehabilitation, decontamination projects change from open pit to block cave, change from open pit to underground etc. 	<p>You should:</p> <ul style="list-style-type: none"> Conduct a mine, mine plan and design review to identify high level risks Review available risk assessment documentation Select sample of high risk areas and audit mine to ensure controls in place Review audits, incident reports and investigations and determine: <ul style="list-style-type: none"> Quality of recommended corrective actions If actions are in place <p>For divestments, you should:</p> <ul style="list-style-type: none"> Ensure that risk assessment documentation is available Identify areas of potential environmental contamination and: <ul style="list-style-type: none"> Determine legal responsibility for clean up Determine financial impact to Owner.



Element 1 – Establish the Framework

Existing Operations

The intent of the Guideline is that all existing operations should conduct initial detailed hazard studies and then conduct hazard study reviews on a five-year cycle. In some countries this is a legislative requirement.

Some sites may never have undertaken any form of hazard study review. For these, the high-level facility review should be a priority. This will allow them to set priorities for further detailed studies in a way that does not overly stretch resources. For newer sites that have had comprehensive studies applied during the design process, the cyclic review process need only be applied.

Changes to Existing Operations

Change management should be a central component of any site health and safety management system. The intent is to ensure that well meant changes – whether temporary, permanent or of an emergency nature – do not have adverse impacts on the integrity of the operation or its protection and prevention systems. Changes to be controlled include mine planning, mining methods, management structures, operating procedures and labour arrangements – in short, any change that could impact on health and safety.

New Projects

For new projects, including expansions to existing operations, formal hazard studies applied throughout the project life are proven and widely accepted ways of maximising inherent safety and minimising risk. Additional benefits include reduced commissioning time, increased operational availability and fewer plant outages.

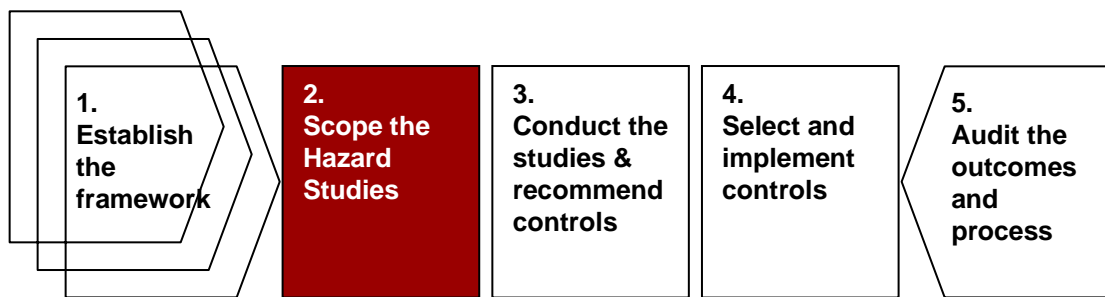
Acquisitions & Divestments

For acquisitions, the intent of the Guideline is to ensure that there is an appropriate level of health, safety and environment assessment before the final decision is made to purchase. The objective is to ensure that the company does not purchase unknown problems. The results may be used to influence the decision to acquire, to influence the purchase price, or ensure appropriate allowance for remedial works post-purchase.

A similar intent implies to divestments. In many countries, responsibility for environmental clean up does not pass to the purchaser. Similarly, responsibility for poorly designed operations may stay with the previous owner. Appropriate hazard studies and investigations prior to selling an asset can help the company manage exposure and provide a level of assurance for prospective purchasers.

TABLE 5.3 – STEP 2 SCOPE THE RISK ASSESSMENTS

	Select Methodology	Define Parameters	Identify Information	Select the Team
Standard	Match the rigour of the method to the risk of the system being studied. Eg for mining alumina the risks are significantly less (and different) to block caving.	Define the purpose, boundaries, and consequences of interest, external interests and any assumptions.	Identify information requirements and obtain appropriate documentation.	Select a team with the appropriate experience, authority, training, expertise and credibility.
Requirements	<p>You should:</p> <ul style="list-style-type: none"> • Ensure that any tasks, procedures or plant areas assessed as high risk eg shaft sinking, initial caving etc are subjected to the most rigorous risk assessment methods (eg. JSA, PHA, FTA, ETA, HAZOP, FMEA or a combination) • Use less rigorous risk assessment methods for lower risk areas (eg. What-If/Checklist) • Use crew-based tools for task-level assessments (eg, Job Safety Analysis). 	<p>Consider:</p> <ul style="list-style-type: none"> • Purpose – eg. Identifying Hazards that could cause damage to people, plant or environment • Physical and process boundaries – the limits of where you will be looking for hazards • Consequences of interest – site generic or mine project specific levels of concern • External influences –outside influences that may have implications within the study boundary eg proximity of neighbours, water bodies, old workings, regulators, legislation, Company policies • Assumptions – features of the area or process to be studied which can reasonably be assumed. 	<p>All studies will require:</p> <ul style="list-style-type: none"> • Appropriate drawings to show the plant, equipment and mine layout (P&ID's, layouts, GA's,) • Appropriate brief description of the process/facility • Detailed geotechnical data • Detailed historical data • Data from similar mine operations on hazards and risks <p>Consider the following supporting documentation:</p> <ul style="list-style-type: none"> • Specification sheets • Detail drawings • Manufacturers data • Equipment specifications • Incident reports • Operations and maintenance manuals • Photographs • Infrastructure design • Construction plans • Commissioning plans • Hazardous materials data • Commodity data • Access plans 	<p>You should:</p> <ul style="list-style-type: none"> • Include an independent trained leader • Include people who have expertise and experience with the area or process being studied, including the various models of operation • Include an experienced scribe to document the risk assessment meetings.



Element 2 – Scope the Hazard Studies

Select Methodology

The methodology chosen should be appropriate to the risk level associated with the plant or facility. The hazard study leader should be instrumental in choosing or vetting the methodology. Higher risk facilities should have rigorous team based methods applied, such as HAZOP or What-If. / Checklist reviews may be more appropriate for low risk facilities.

The method should also vary depending on the type of system being studied. HAZOP is appropriate for complex processing systems, but JSA may be more appropriate for examining a specific task or operation. Combinations of methods should also be considered when appropriate.

Refer to the chapter on Risk Assessment for information on how risk matrices may be used to help guide selection of appropriate methodologies.

Define Parameters

Setting boundaries and identifying a clear purpose are essential to any study. The consequences of interest should also be defined – is the study focusing only on safety, or also on environment and operations? What will be the threshold risk level, below which no action will be taken?

Identify Information

Once the information requirements have been defined, the required documents need to be gathered. It is usually sufficient for one copy to be available to the team, often in the hands of the most appropriate discipline engineer or operations representative.

The key study documents, for example P&ID's or mine plans, should be available in large print for all to see, or in sufficient number. If multiple sets are provided, one should be marked as the master set for any markups made during the study.

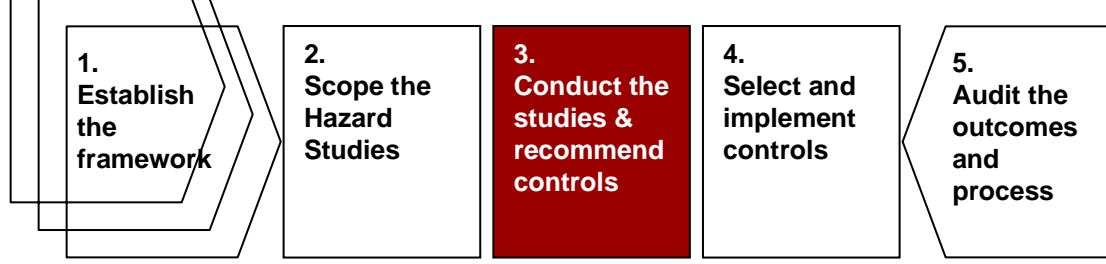
Select the Team

The team should include appropriate discipline engineers (mechanical, process, electrical, mining, control, etc) where they are relevant to the facility. Representatives of operations supervision and operations/maintenance technicians should also be included. Usually one of the team also fulfils the role of scribe.

Technology suppliers and equipment vendors should be included when appropriate. Other outside stakeholders may be included, although the general rule is that they should add value to the study, not be passive spectators.

TABLE 5.4 – STEP 3 CONDUCT THE STUDIES

	Prepare	Conduct	Recommend Controls	Document
Standard	Team members, scribe, leader and sponsor should be involved in appropriate preparation prior to the study.	Conduct the study using an agreed, recognised methodology.	For each identified hazard with consequences of concern, identify appropriate control measures.	Ensure that the entire risk assessment is appropriately documented using an accepted method.
Requirements	<p>Leader and sponsor should:</p> <ul style="list-style-type: none"> • Circulate appropriate background information • Determine appropriate section or node break points appropriate to the study method being used • Ensure team members have appropriate training • Ensure venue is appropriate to the type of study and number of participants • Ensure that interruptions will be minimal during the study • Set a timetable for study sessions. 	<p>Refer to texts, previous training material or later discussion, articles, for:</p> <ul style="list-style-type: none"> • Hazard & operability studies (HAZOP) • FMEA • What-If/Checklist • FTA/ETA • JSA • PHA • WRAC <p>The risk assessment leader is primarily responsible for ensuring that the method is appropriate and is properly applied.</p>	<p>Consider the hierarchy of controls. Solutions from higher up the list are preferable, for critical risks more than one type of control is needed:</p> <ul style="list-style-type: none"> • Eliminate the hazard entirely • Reduce the consequences of the hazard • Reduce the likelihood of the hazard • Protect the person, plant or environment from the hazard • React rapidly to limit the impact of the hazard when it occurs • Provide optimum repair and recovery after the event <p>Refer to Haddon’s strategies for other ideas (see earlier in text).</p>	<p>Issues to cover include:</p> <ul style="list-style-type: none"> • Reasoning behind the selection of risk assessment method • A record of scope • Assumptions behind the choice of sections • Methodologies employed • Team members • Minutes of meetings, including hazards, potential consequences, safeguards and actions • Timing of the study • Actions • Sign off list for completion of actions from the study • Develop hazard register



Element 3 – Conduct the Studies

Prepare

The bulk of the preparation will be done by the hazard study leader and the study sponsor. Others can prepare by ensuring that they understand the reasons for the study, the project background and how the operation being studied works. The leader or sponsor may circulate relevant information, such as past incident reports, to team members to get them thinking about how things might go wrong.

Conduct

The hazard study leader will be primarily responsible for the conduct of the study. His or her role will be to ensure that the method is applied appropriately, any changes to established methods are justified and documented, and that appropriately detailed minutes are produced. All team members can assist by keeping to schedule with start and break times and minimising interruptions. Hazards are initially identified by ignoring existing or already proposed controls and safeguards.

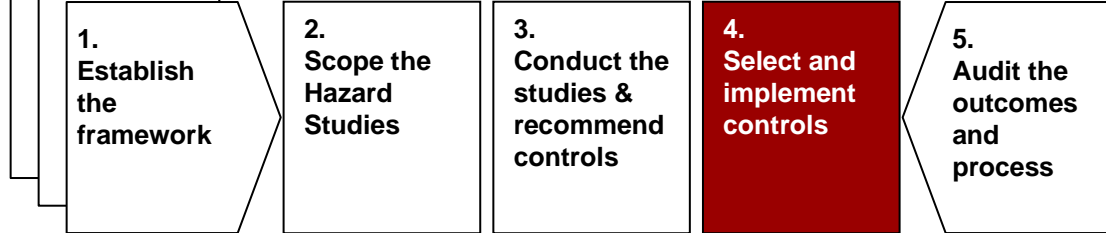
Recommend Controls

The primary aim of the study is to identify and clearly define (document) hazards, not necessarily to identify solutions and controls. However, once a hazard has been identified and the existing/already proposed controls assessed as inadequate, appropriate controls will often be readily apparent and can be defined by the team during the study. For controls that need to be defined after the study, appropriate mechanisms should be in place to ensure that they are appropriate to the hazard and do not introduce new hazards.

Document

For team based studies, the primary documentation will be the minutes of the meetings. These should be supplemented by clear notes and memos detailing work done in following up identified hazards.

A report should be prepared covering the issues outlined in the table for Element 3. Sites should establish a standard format and content for such reports. In some countries, hazard study reports for new projects or cyclic reviews must be submitted to statutory authorities and so must comply with their requirements.



Element 4 – Select and Implement Controls

Set Priorities

Risk assessment can be used to assist with setting priorities – refer to the chapter on Risk Assessment for further information. Other factors that may be important in setting priorities and timeframes include: need for a shutdown; capital cost versus capital available; technical feasibility of solution.

In situations where the consequences of a hazard can be expressed readily in financial terms, a cost-benefit analysis may be useful. Note that while cost-benefit analysis is attractive to insurers, it does not take into account the cost of human suffering and should not be used as a primary decision criterion for safety or health related hazards. For further details on cost-benefit, refer to the chapter on Risk Assessment.

Implement

Once the priorities are set implementation should proceed accordingly. Some actions or recommendations will require further studies or will be projects in their own right. Others will require the study sponsor to manage them and ensure that they are completed.

Part of the implementation should include:

- Inspection for safety and completeness before commissioning (as appropriate – this may mean a physical inspection in the field for a plant-based action, or review of a new procedure before publication)
- Review to ensure that all related documentation (drawings, procedures, forms, etc) have been updated as appropriate
- Post-commissioning audit, to ensure that the objectives of the action are being met

Communicate

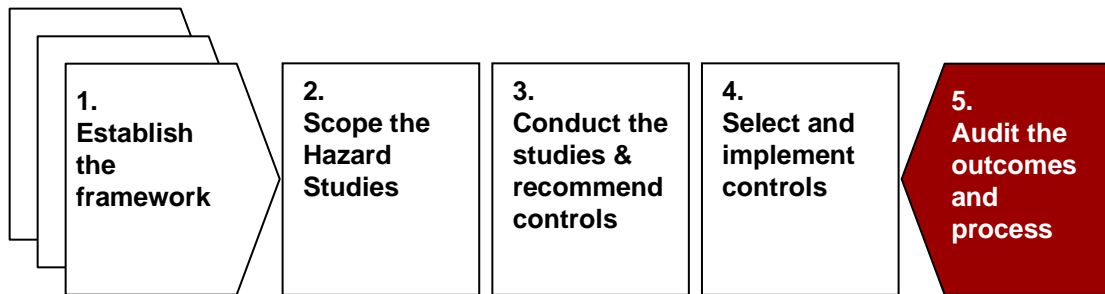
Of particular importance is the need to train operators and technicians if the action requires them to work in a different manner or with new or modified equipment.

TABLE 5.5 – STEP 4 IMPLEMENT THE CONTROLS

	Set Priorities	Implement	Communicate
Standard	Review the recommended actions and controls and set priorities based on assessment of risk, ease of implementation availability of resources, and availability of access to mine facility.	Implement actions as recommended by the risk assessment, according to priority and schedule.	Ensure that all appropriate stakeholders are informed of the outcome of the study. Ensure that all persons affected by an action are informed of the impact beforehand.
Requirements	<ul style="list-style-type: none"> • Changes to planning and design can readily be implemented, changes to existing mines will be more difficult and costly. • Where long term risk control will take time to implement, ensure that short term risk controls are implemented in the meantime • Document the implementation schedule and the reasons for priority settings. 	<ul style="list-style-type: none"> • If deviating from a recommended action: <ul style="list-style-type: none"> • Clearly define the reasons why • Clearly demonstrate that the alternative is equally safe or better, or why the action is no longer necessary • Ensure other affected systems are changed where necessary, including <ul style="list-style-type: none"> • Emergency response • Maintenance procedures • Operating procedures • Inspection schedules • Company standards (including engineering and safety) • Training • Induction • Mine and infrastructure designs and drawings. • Carefully manage any actions to ensure that they, in turn, do not introduce new hazards or increase risks <ul style="list-style-type: none"> • Record progress and completion of implementation. 	<p>Consider the following:</p> <ul style="list-style-type: none"> • Affected employees – communicate the hazards identified in the area or task, and the controls to minimise the risk • The study team – feedback the recommendations that were implemented and suggest any improvements for their process • Other sites – share a knowledge of critical risk with other mine operations that are known to use similar equipment or tasks • Regulatory/statutory Government bodies and Inspectors • Any others who need to know about the results, eg. contractors, local community

TABLE 5.6 –STEP 5 AUDIT THE OUTCOMES AND PROCESSES

	Study Follow-up	Risk assessment Audit	System Audit	Improvement
Standard	For each study, ensure that appropriate follow-up meetings are held until all action items are properly resolved and documented.	On a regular basis, conduct an internal audit of the quality of risk assessments being conducted within the organisation.	On a regular basis, conduct an external audit of the entire system for hazard management within the organisation.	Based on the results from audits and individual studies, define and implement improvements to the hazard management system within the organisation.
Requirements	<p>You should:</p> <ul style="list-style-type: none"> • Conduct regular review meetings for each study • Conduct a close-out (final) review meeting and document it • Ensure that all actions have been implemented • If actions have not been implemented, ensure that the reasons for this are valid and are clearly documented • If different actions have been implemented, ensure they are validated and documented • Ensure that all actions have been reviewed to ensure that they do not introduce any new hazards 	<p>You should:</p> <ul style="list-style-type: none"> • Audit a representative sample of risk assessments • Ensure sample covers most risk assessment types and most risk assessment leaders • Use a trained auditor and risk assessment leader for the audits <p>Audit the following aspects:</p> <ul style="list-style-type: none"> • Methodology selection • Methodology application, especially deviations • Effectiveness of recommended controls • Team selection and composition • Leader selection and performance • Quality and thoroughness of study minutes • Implementation of actions • Follow-up process 	<p>You should:</p> <ul style="list-style-type: none"> • Use a recognised and qualified external auditor (i.e., from outside the particular organisation) • Audit the system for risk assessments, including application to: <ul style="list-style-type: none"> • Existing mining facilities • Changes to existing mine facilities • New mine projects • Acquisitions & divestment • Audit a selection of studies, as outlined under “Risk assessment Audit” • Audit the internal audit processes • Audit implemented actions to ensure they are still in place • Audit the close-out of studies, including updating of documentation and training of operators • Audit the improvement and feedback loop 	<p>You should:</p> <ul style="list-style-type: none"> • Keep track of all recommendations for improvement by source and date • Review the merit of all recommendations • Implement recommendations in a timely manner • Ensure that valid reasons are given and documented for rejecting any recommendations • Establish a system and review process to track progress of implementation of recommendations <p>Consider:</p> <ul style="list-style-type: none"> • A single database for all improvement recommendations • Combining with a site-wide “HSE Plan” for all HSE improvements and actions • Including actions from individual risk assessments in the same system



Element 5 – Audit the Outcomes and Processes

Study Follow-up

Thorough follow up of hazard studies to ensure that actions are implemented fully and in a timely manner is essential. The best hazard study is useless unless the recommended actions are implemented.

For small studies, it may be appropriate to keep track of the relatively small number of actions informally until they are mostly complete. A formal review meeting should then be held and the actual actions taken noted. The review meeting should consist of a representative sample of the original study and should ensure that the implemented action meets the intent of the study and does not introduce any new hazards. The formal review meeting should be documented and the report/minutes filed with the hazard study report.

For larger studies, a number of formal review meetings may be appropriate. Each should review progress of outstanding actions and review actions completed since the last review. Completed actions should be reviewed to ensure that they meet the intent of the original hazard study and do not introduce new hazards. Each meeting should be documented and they should continue until all actions are completed.

Hazard Study Audit

This can be done internally. The auditor should be a senior person within the organisation with hazard study leadership expertise. Management systems should ensure that findings from the audit are acted upon so that the process is improved.

System Audit

As part of overall external auditing of the site's safety program, an audit of the entire hazard study system should be undertaken. The auditor should have credibility in hazard studies and should be tasked with finding opportunities for improvement in the system, rather than simply trying to find non-compliant hazard studies.

Improvement

To ensure that the audits and review lead to an overall improvement in the quality and efficiency of hazard studies, there should be a mechanism in place to track all improvement suggestions. This should be reviewed at a senior level regularly.

TABLE 5.7 - EXAMPLE 1 – NEW PROJECT OR MAJOR UPGRADE

	Element 1: Establish the Framework	Element 2: Scope the Risk assessment	Element 3: Conduct the Study	Element 4: Implement Controls
Timing	The framework for risk assessments should be discussed and agreed at project inception. They should be built in to plans, timetables, cost estimates from day one.	For each risk assessment, the scope should be defined as early as possible. Generally the scope is set approximately a month prior to each study.	Conduct the studies at a time when the required information is available and that best allows actions arising from the studies to be incorporated in to the design process.	Incorporate actions arising from each risk assessment into (as appropriate): design procedures & standards; design details; construction, commissioning or operating procedures
Typical Activities	<ul style="list-style-type: none"> Establish or adopt safety policy for the project Acquaint key personnel with company & statutory HSE requirements and standards for geotechnical design and financial issues Identify specific HSE-related studies required by statutory authorities Determine which risk assessments are required Estimate time and cost of risk assessments Obtain agreement from senior project and company management, committing to the risk assessment process Identify and source tools to be used, including checklists and software Identify training needs for prospective risk assessment team members Identify and engage any external expertise required, such as risk assessment leader 	<p>For each study;</p> <ul style="list-style-type: none"> Identify team members early Secure appropriate location Ensure team members are sufficiently trained Define study boundaries and objectives Appoint leader and scribe and involve leader in team selection and scoping of study Review results & status of previous study/studies Prepare and issue briefing document covering above, at least three weeks prior to first risk assessment session Develop preliminary hazard inventory for full range of hazards not just HSE 	<p>For each study:</p> <ul style="list-style-type: none"> Ensure accurate minutes are recorded Keep study sessions short – less than two hours between breaks and no more than seven hours in-session per day Conduct sessions without interruptions Document and justify any deviations from established risk assessment methodology Mark-up relevant documents and drawings to show areas studied and recommended actions and keep as part of meeting record Review previous day’s results at the start of each day 	<p>For each study:</p> <ul style="list-style-type: none"> Develop an action plan Establish target dates for completion Assign individual accountability for each action <p>Use Element 5 – Audit the outcomes, to ensure that actions are closed out in a timely manner.</p>

TABLE 5.8 - EXAMPLE 2 – EXISTING MINE

	Establish the Framework	Scope the Risk assessment	Conduct the Study	Implement Controls
Timing	Retrospective risk assessments can be applied at any time to an existing mine and mine plan as part of a hazard management program.	For each study, the scope should be set approximately one month in advance of the study, to allow time for preparation.	Timing of risk assessments will be dependent on the availability of resources, which in turn is dependent on management commitment to the process.	Actions will either require physical plant changes or changes to procedures for operation, maintenance, and training. Timing should be as soon as practicable.
Typical Activities	<ul style="list-style-type: none"> • Determine/obtain management commitment to retrospective risk assessments • Determine program of risk assessments, starting with mine, mine plan and design review • Estimate time and cost of risk assessments and establish a time table • Identify and source tools to be used, including checklists and software • Identify training needs for prospective risk assessment team members • Identify and engage any external expertise required, such as risk assessment leader or trainer • Ensure that necessary documentation is up to date. For a processing facility, as-built P&IDs and other drawings are required; for a mine the design parameters and plans will need to be confirmed 	<p>Generally consider undertaking the following studies:</p> <ul style="list-style-type: none"> • Facility Review • Detailed HAZOP and What-If studies and/or, if appropriate, FTA, ETA, FMEA studies <p>For each study:</p> <ul style="list-style-type: none"> • Identify team members early • Secure appropriate location • Ensure team members are sufficiently trained • Define study boundaries and objectives; HSE, Financial, geotechnical, methods, equipment • Appoint leader and scribe and involve leader in team selection and scoping of study • Review results & status of previous study/studies • Complete preliminary hazard inventory • Prepare and issue briefing document covering above, at least three weeks prior to first risk assessment session 	<p>For each study:</p> <ul style="list-style-type: none"> • Ensure accurate minutes are recorded • Keep study sessions short – less than two hours between breaks and no more than seven hours in-session per day • Conduct sessions without interruptions • Document and justify any deviations from established risk assessment methodology • Mark-up relevant documents and drawings to show areas studied and recommended actions and keep as part of meeting record • Review previous day’s results at the start of each day • Conduct inspections of the facility as required to ensure understanding of the as-built condition 	<p>For each study:</p> <ul style="list-style-type: none"> • Develop an action plan to implement controls and modify mine plan and design • Establish target dates for completion • Assign individual accountability for each action <p>Use Element 5 – Audit the outcomes, to ensure that actions are closed out in a timely manner.</p>

TABLE 5.9 - EXAMPLE 3 – CHANGES ON AN EXISTING FACILITY

	Establish the Framework	Scope the Risk assessment	Conduct the Study	Implement Controls
Timing	<p>A procedure and process for management of change should exist on all sites.</p> <p>All personnel should be trained to an appropriate level of detail in the change management process.</p>	<p>Effective change control relies on early identification of a proposed change followed by appropriate review and analysis of the change for HSE and financial implications, followed by formal approval.</p>	<p>The time for completion of each step in the change management process will depend on the nature of the change and the urgency assigned to. No change can be so urgent that it cannot be properly assessed and approved.</p>	<p>Controls arising from review and assessment of change proposals will require the proposal itself to be modified or additional training, procedures or plant items to be provided. All such actions should be implemented prior to implementation of the change.</p>
Typical Activities	<ul style="list-style-type: none"> • If not already existing, establish a change management procedure, provide training and monitor compliance • As part of the procedure, established the following: <ul style="list-style-type: none"> • Change register • HSE checklist to review change proposals • Guidelines for level of effort to apply to assessment of proposals • Forms to document change proposals and approvals • Process to ensure that maintenance activities that involve changing plant are not carried out without an approved change proposal <p>(“Changes” can also be referred to as “modifications”.)</p>	<p>For each change or modification:</p> <ul style="list-style-type: none"> • Describe the proposed change and provide justification or reasons for the change • Review using an appropriate HSE, financial and geotechnical checklist • Review by experienced plant personnel for suitability • Determine type of detailed study, if any, that change proposal needs to be subjected to. • Formally approve the change for further examination, or reject the change and provide reasons • If approved, scope the risk assessment – refer to Examples 1 and 2 	<p>Refer to Example 2.</p> <p>Once the study is complete, the change proposal, as modified following the study, and the results of the study should be submitted for final approval.</p> <p>Authority to approve changes should be vested in appropriate managers or engineers in writing by the senior manager on site.</p>	<p>Recommended actions arising from any risk assessment of a proposed change should be managed in the same way as Example 2:</p> <ul style="list-style-type: none"> • Develop an action plan • Establish target dates for completion • Assign individual accountability for each action <p>All actions should be appropriately addressed before final approval for implementation or operation of the change is granted.</p>

5.11: Generic 6-Stage Hazard Study Process

This section is a discussion on a project process for ensuring hazards are identified and managed at all appropriate stages of the project. It is taken from the chemical/oil industry where it is used in various versions and has been successfully translated into the mining industry. It was originally developed by ICI in the UK.

Introduction

It is apparent from the study of many disasters that a major contributing element was either a failure to identify the hazards or a failure to act when hazards were identified. In the former category there is Flixborough (explosion), BHP mine (explosion), Bhopal (toxic gas), Coode Island (fire) and "Herald of Free Enterprise" (sinking). In the latter category is London Underground (collision), Piper Alpha platform (fire, explosion), Phillips (fire, explosion), and Challenger ('O' ring failure). These are the spectacular front page headline grabbing incidents, there are many others that result in a disaster, only the scale is different. All, without exception, were avoidable.

Another feature of all these incidents was a lack of any systematic approach to risk management. None of the facilities had a functioning safety management system in place. If there had been functioning systems, of which hazard studies are but a part, it is likely that the disasters would not have happened.

By using a systematic process for hazard identification and minimisation at all stages of a project, such failures can be avoided. A Hazard Study process will help to ensure that a project progresses from preliminary feasibility study through to beneficial operation with the minimum of hazards built-in and clearly defined safety management requirements. By identifying issues early, a sound Hazard Study process ensures that the design, construction and commissioning of the facility progress with minimal delay and rework. At the end, the Hazard Study process provides a detailed safety dossier for the facility with an auditable trail of the decision making process.

The Hazard Study process is of itself simple; the application requires management commitment and multi-disciplinary skills of a high order, along with a long term commitment to ensuring all activities are carried out with minimum and managed risk.

The Hazard Study Process

To ensure all hazards are identified and adequately managed it is necessary to have a very practical design process that forces the issues to be addressed. The following is an outline of such a process that uses multi-disciplinary team skills integrated into the process. There is a need for a corporate long term commitment to ensuring all activities involving hazards are carried out with minimum and managed risk. Although there is clearly a cost involved in following such a process, it is demonstrable that facilities designed using such a process cost less overall than those not using such a process. The savings come from imposing design requirements early, identifying potential problems early, having a trouble free startup of the facility and ongoing significant operational efficiencies. Comparisons suggest a full cost recovery within six months of startup and recurring significant savings over the life of the facility that would not otherwise be achieved.

In addition to all the typical design procedures that would be applicable to a new facility or upgrading/modifying an existing facility, risk management strategy requires close attention to the control of hazards, preferably by elimination. This is done by the application of an integrated group of distinct formal studies and reviews, initiated at the very early stages of project development and carried through to beneficial operation. The scope and extent of

the studies and reviews is dependant on the hazardous nature, complexity, and size of the project involved. That is, the studies are tailored to suit.

In the following text, the Hazard Studies are described in relation to a new facility. With little change except scale, they can be applied to any modification on an existing facility. Further, by applying these studies in retrospect to an existing facility a clear measure of the shortfall between what is required and what exists can be derived, allowing suitable action plans to be developed and implemented in coordination with budgetary restraints.

It should be noted that this paper outlines a generic process. The scope of any studies for a specific project need to be appropriate to the complexity and probable hazards of the project

The timing of the hazard studies is shown in Figure 5.10. The studies are discussed below.

Hazard Study 1

This first study is carried out during the initial feasibility study phase and its purpose is to ensure that the understanding of the project, the process, and the materials involved is sufficient to enable all health, safety and environment (HSE) issues to be properly assessed. Where information is found to be lacking, the study initiates further work to obtain the required data. It contributes to key policy decisions and ensures that contacts are established with all parties, internal and external to the company, who may contribute to or impose constraints on the development of the project.

The study is carried out by a multi-disciplined team, usually including a representative of the business group (owner), project manager, site representative, process engineer, occupational hygienist, environmental specialist and possibly technical specialists as appropriate. The team is lead by an independent, trained and experienced study leader who is responsible for the quality of the study and the report.

This study identifies all the applicable regulations, legislation, and company standards. It should be initiated and driven by the owner (Project Leader).

The study will generally consider:

- Definition of project objective and scope
- Reviews of incidents on similar facilities
- Collection of data on safety, health and environment
- Reviews of draft environmental impact statement
- Identification of all relevant international, national and company HSE standards
- National legislation and regulatory approval HSE requirements (such as quantitative risk assessment (QRA) and Hazard and Operability (HAZOP) Study)
- Criteria for health, safety and environment; define project criteria
- Standards required to meet anticipated regulation and codes of practice
- Appropriate routing for transport
- On and off site materials transport
- Waste minimisation and recycle proposals
- Energy and resource conservation measures
- Human and organisational aspects of project proposals
- Further study timing and need for QRA, Control System HAZOP etc.
- Any other relevant issues.

The tools used in this study may be checklists, pro-forma or What If? type analysis.

Hazard Study 2

This study is carried out during the definitive feasibility study phase, usually during conceptual engineering design. The purpose of this study is to identify significant hazards and provide the opportunity for their elimination by re-design. If this is not practicable, measures may be incorporated to meet the relevant criteria. This study produces most of the information and assessments needed to meet the requirements of regulatory authorities on safety, health, and environmental protection.

The study is carried out, again, by a multi-disciplined team of the project manager, process engineer, operations representative, process control engineer, and again an independent, trained, study leader.

The study considers:

- Any impact (health, safety, and environment) which the project may have on or off the facility
- Any significant hazards, including loss of containment which could result in toxic flammable or explosive hazards. Formal hazard identification processes are used
- Changes to process conditions which could lead to consent levels for discharge being exceeded
- Completion of preliminary risk assessment/hazard analysis
- Measures proposed to prevent exposure to chronic or acute health hazards
- Preliminary safety studies are completed (fire risk management, other natural events, etc.)
- Information which will be used for other studies and design procedures (pressure relief, trip and alarm testing, etc.).

This study is initiated by the Project Manager or the owner (Project Leader).

The tools which might be used at this stage are Process Hazards Analysis, Checklists, What If? analysis, Fault Tree Analysis, Event Tree Analysis, experience etc.

Hazard Study 3

This study is carried out to review the facility design and procedures to identify any hazards or obstacles to operability which could arise, particularly through deviations from the design intent. This is usually carried out towards the end of the front-end engineering. The consequences of deviations are identified and where necessary appropriate corrective actions initiated (hardware and/or software).

The team for this study is similar to that used in Hazard Study 2 plus any specialists required.

The study includes:

- A detailed systematic study of the design and outline operating and maintenance procedures to identify the consequences of deviation from design intent
- Consideration of transient conditions during startup, shutdown, facility upsets, and emergencies
- Consideration of potential exposure of employees to chemicals during operations
- Control system hazard study
- Development of fire safety and other natural peril requirements.

This study is initiated by the Project Manager.

The tools used in this study is most typically HAZOP (Hazard and Operability) Study. It could include FMEA, What If, Checklist, FTA, ETA, etc.

It should be noted that all changes to the design made after this study need to be subject to the same level and rigour of study as has been applied at this point. Formal change control methods should apply from this time.

Hazard Study Review

This review is intended to check that the facility as designed meets the design intent and to check all Hazard Study 1, 2 or 3 actions have been incorporated. It also checks operating instructions and emergency procedures comply with any requirements identified by earlier hazard studies and are appropriate.

The review is carried out by the commissioning manager or operations manager of the facility concerned and co-opted staff and is completed prior to the start of commissioning.

The review includes checking:

- Actions from earlier studies are complete
- Documentation is complete
- HAZOP and other Hazard Study 3 issues are complete
- Detailed occupational health assessment is available
- Operating procedures for all potential operational situations are complete and realistic
- Emergency procedures are available and complete and exercises are run
- Review of audit procedures for safety systems. Initiate audits as required

The tool for the Hazard Study Review is a generic audit process aided by appropriate checklists for procedural issues.

Hazard Study 4 (Construction Safety Study)

A construction safety study is carried out towards the end of design and prior to construction and the intention is to identify how all the construction hazards will be managed. It addresses the following questions:

- What are the possible potential hazardous incidents that could occur during the proposed construction that could affect existing plant, personnel or environment?
- What are the possible potentially hazardous incidents that could occur during the operation/maintenance of the existing plant, that would affect the construction personnel, construction program or the environment?
- What are the management policies, systems and work instructions set in place for the existing plant and the construction activity to minimise or eliminate the chance of an incident occurring?
- Have procedures been developed and set in place to cover all emergencies that might arise during construction?

A useful tool that may be used to identify the issues that must be addressed in this review is the brainstorming 'What If?' technique. This can be used to investigate all aspects of construction and identify what problems might arise.

The team involved would be brought together from the operating group, the commissioning group, and the construction team. The team would be led by the hazard study leader and a formal report generated on how the interface with the pre-existing or future operations and the construction will be handled. It also details how the construction activity will be managed — procedures used etc.

The output formalises the relationship between construction and pre-existing operations and provides the basis of the construction safety management plan at the interface and within the construction area by identifying all the procedures required to manage the issues.

Hazard Study 5

The purpose of this study is to provide an opportunity to ensure that the implementation of all personnel safety, employee health, environmental protection, and risk management issues is appropriate to meet all company and legislative requirements.

The study is led by the commissioning manager/production manager with a team comprising the project manager, commissioning manager, operations safety adviser, operators' HSE representative/delegate, occupational health specialist, and environmental adviser.

The study takes place immediately prior to the start of commissioning and is updated at the end of commissioning.

The study covers:

- A review of the protection of employee health including ongoing monitoring
- A review of the arrangements for employee safety
- A review of equipment and systems provided to protect the environment and for monitoring environmental performance.

The study is initiated by the Commissioning Manager/Production Manager.

Post Start-up Hazard Management Review and Audit

The purpose of this review is to ensure that the issues raised in the previous studies have been brought to an appropriate conclusion and the appropriate documentation exists in the facility records.

It is also charged with reviewing early operation to ensure it is consistent with the design intent opposite safety, health, and environmental issues and that assumptions defined in the earlier studies are borne out in actual plant operation. Any operating and maintenance difficulties identified are fed back to the group responsible for the design.

This is a key opportunity for learning from experience for the design group.

The study team meet to consider issues raised by considering systematically the points below.

- Review operating experience (versus design concept)
- Review changes made during commissioning and start up for significant hazard implications and ensure they were appropriately evaluated and that facility documentation and operating instructions have been updated

- Occupational Health : Review results of any monitoring, exposure of operators and frequency of leaks, spills, emissions, and check that they are in line with the original assumptions.
- Environment : Review performance against any consent levels, continuous and abnormal discharges.

The study team would include the following or someone of similar status and knowledge.

- Commissioning manager/operations manager
- Facility manager
- Project manager
- Hazard Study leader
- Environmental specialist
- Occupational health specialist

The team would be convened by the commissioning manager or the facility manager. For the audit of the safety management system there would probably be a team of:

- Lead auditor
- Support auditors

The number of the latter involved would depend on the size and complexity of the facility.

The timing of the study would be between three and six months of the facility achieving beneficial production.

Design Impact

From the descriptions of the contents of each hazard study and review it is apparent that undertaking hazard studies is inextricably tied up with the design process. The studies help formalise and provide rigour to processes that might or might not be carried out under a different project design regime.

Figure 5.11 shows how the studies are linked into the engineering life cycle for a facility. Indeed they do not stop when the project is complete and the facility is operational, rather they continue throughout the facility lifetime as every change is assessed.

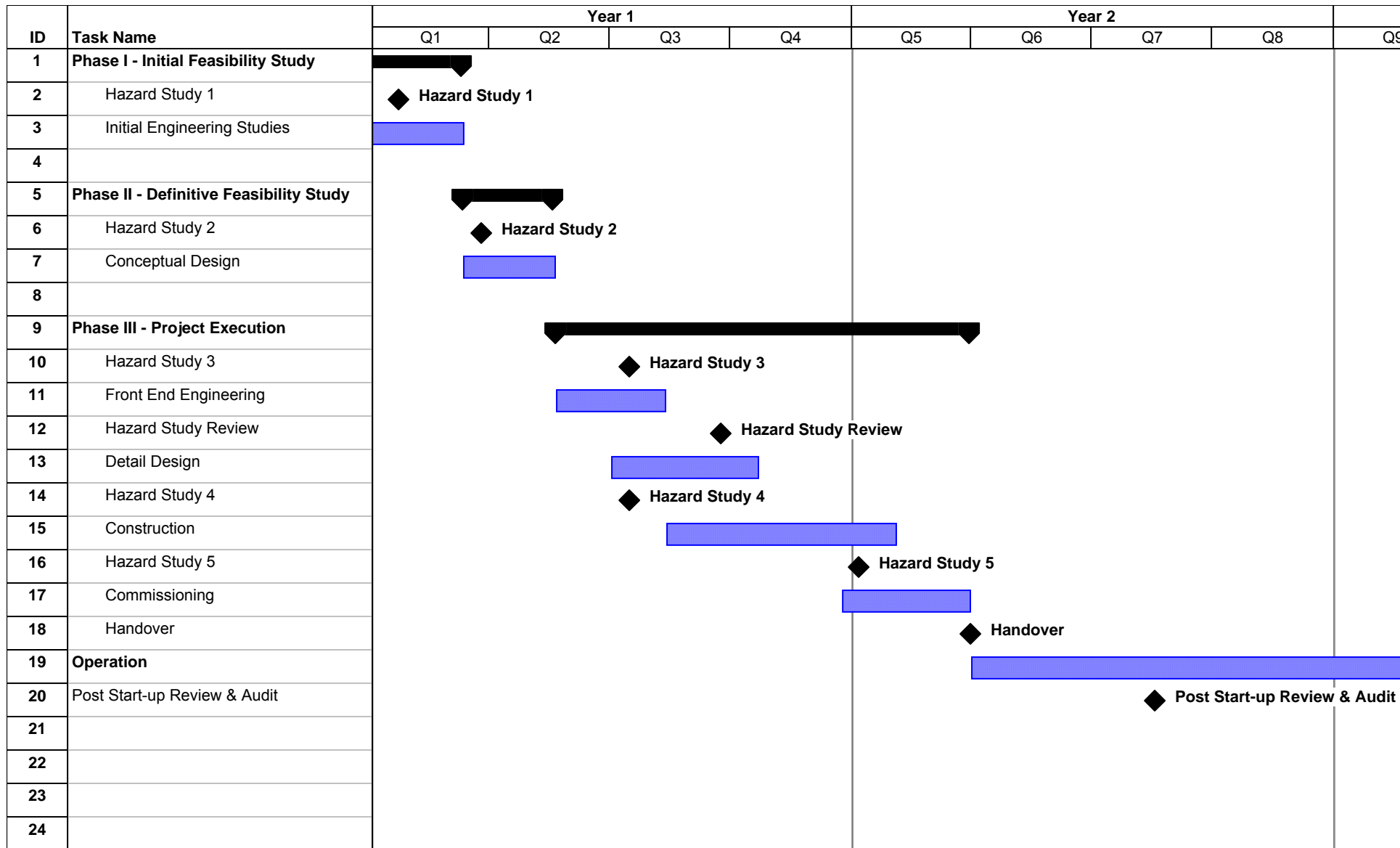


Figure 5.11 Hazard Study Timing

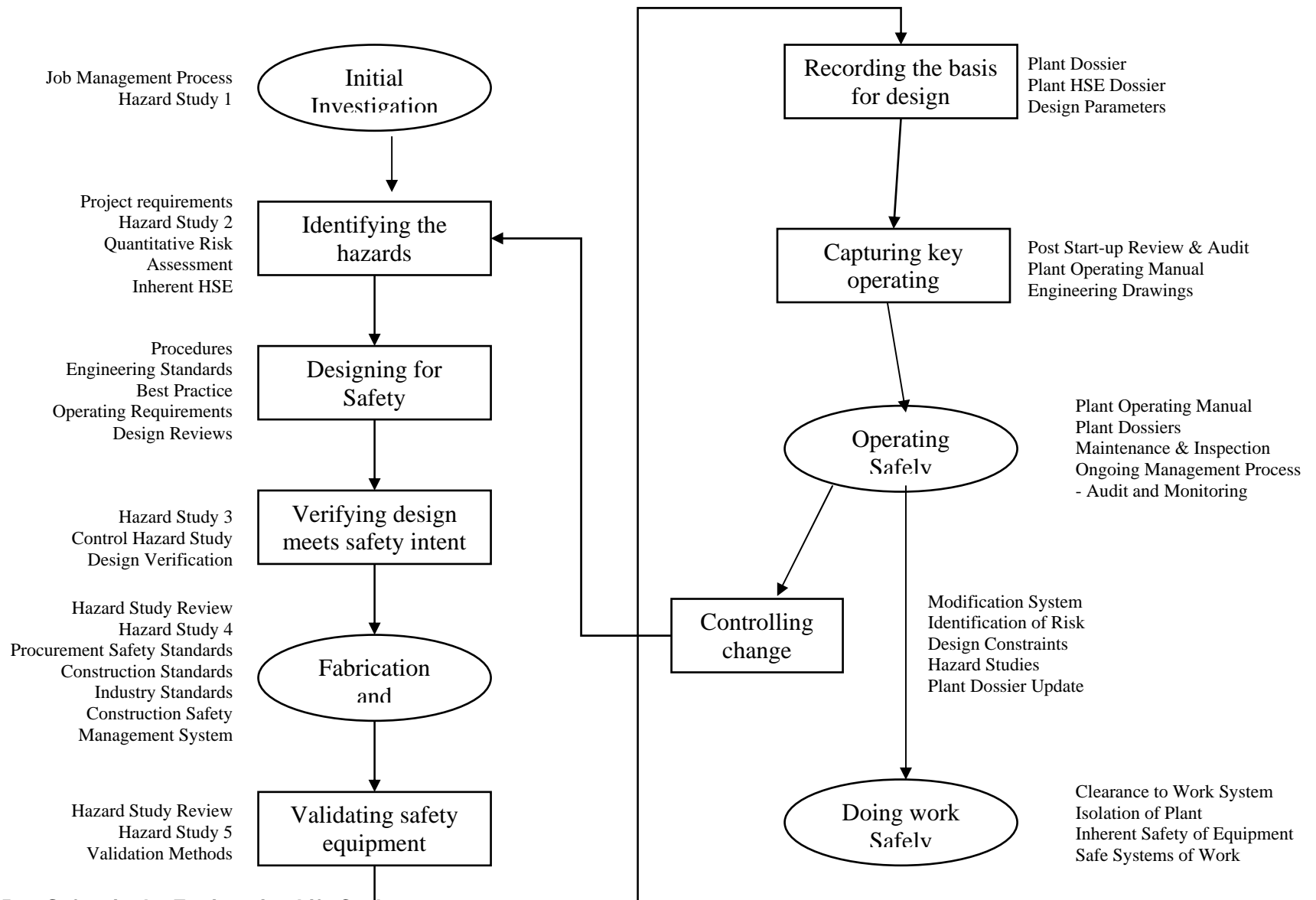


Figure 5.12 Safety in the Engineering Life Cycle

6. Applying the Risk Assessment Deliverables

The expected output of any risk assessment should supply information to address the desired final deliverable, a Formal Safety Assessment, an Operating Plan, a SOP, etc. As previously mentioned, the Scope should define the expected process for utilising the outputs of the risk assessment.

6.1 Documenting the risk assessment process and deliverables

All formal risk assessment should be documented for many reasons including the need for future reference. The specific format will vary depending on the complexity and purpose of the assessment. Minimally, it is necessary to use a scientific approach to the Risk Assessment report such as the following.

Executive Summary

Introduction

Context (strategic, corporate and risk management)

Issues / Reason for Review

Objective

Method

Team (names, positions and related experience)

Hazard Inventory Table

External Potential Impacts

System description and boundaries

Risk Identification Tool

Risk Analysis method

Determination of acceptability, ALARP/SFAP

Documentation used for study

Results (tables, charts, etc.)

Priority risks

Priority existing controls and performance indicators

Priority new controls and performance indicators

Recommended Action (the Action Plan information) including accountabilities and timeline

Note that there is more guidance on report content in NSW Department of Mineral Resources MDG 1010 and 1014.

The draft report should be reviewed by the Risk Assessment client, finalised and, once the required actions have been commenced, stored in a manner that facilitates retrieval and review.

6.2 Deriving the Action Plan

Many Risk Assessments will require that the output include a Risk Assessment Report, as well as an Action Plan listing the suggested new controls and offering an opportunity to identify specific new actions, accountability and target dates.

Table 6.1 Example Action Plan

Hazard Identified	Existing Controls	Recommended New Controls	Specific Action	Accountability	Target date	Completion Date

In the above example the first column, “Recommended New Controls”, would be derived from the Risk Assessment output, possibly by the facilitator or the author of the formal report. The client (or “risk owner”) would ensure the Action Plan was completed.

The final Action Plan should also be include in the formal Risk Assessment report to facilitate traceability.

6.3 Following up on the Action Plan and deliverables

The Action Plan should include an indication of the Completion Date for any new action, as illustrated in the above example. This feature attempts to ensure that required actions are undertaken.

Some mines put their Action Plans into the site project management system and trace completion requirements automatically.

It may be necessary to set an Action Plan review date at some point after the Risk Assessment is completed to ensure all required Actions are complete or on schedule.



THIS IS A KEY ISSUE.

LESSONS LEARNED 6.1

There have been accidents in the minerals industry where an investigation has identified that a previous Risk Assessment has identified the related risk and some required, but incomplete, actions. In this situation the Risk Assessment report becomes the “smoking gun”, indicating that the hazard and risk were understood but the action not taken.

6.4 Using other information from the risk assessment

The Risk Assessment report can provide additional information to the requirements stated in the Objective.

For example, it is desirable to retain information on priority risks from Risk Assessments in ongoing, cumulative site documents sometimes called “**Risk Registers**” see section 4.1.1.B. Even if creating or adding to a site Risk Register is not part of the Objective, some of the output of the Risk Assessment should be retained to help assemble a full site document over time.

6.5 Change Management

The site must have a mechanism to identify changes in hazards or risks that affect past risk assessments, triggered either by regular review of those reports or by some hazard identification process.

Changes to Risk Assessment reports should be noted by revision notation in the document.

This would be a subset of the overall site Change Management Programme that would be covered by the SMS.

6.6 Auditing the Process

Finally, the Context of Risk Assessment should be defined at a site, possibly by a procedure as suggested in Chapter 3 "**Setting the Context**". The defined Context should be used to regularly audit the Risk assessment process to ensure that site activities appropriately reflect the intention. There is an audit checklist example as in Appendix E. It relates to HAZOP specifically but provides clues for other types of study audit.

7.1 Checklists

7.1.1 Scope

Scoping Checklist

A good Scope should include the following:

1. An objective based on the expected deliverable
2. A description of the system to be reviewed and clear identification of the boundaries
3. An inventory of the potential hazards
4. A statement of external threats
5. A listing of assumptions
6. Identification of consequences of interest
7. The risk assessment method – the means of identifying the unwanted events
8. The risk analysis method – the means of calculating and examining the level of risk
9. The facilitator for the risk assessment
10. The scribe for the risk assessment
11. The risk assessment team or work group (identifying reasons for inclusion)
12. The time required (and venue)
13. The means of providing risk assessment results and the desired deliverable

7.1.2 Consultant proposal

Consultant Proposal Checklist

A good Consultant Proposal should include the following:

1. Background information on the issue and the need for risk assessment
2. An objective based on the expected deliverable
3. An overview of the system to be reviewed
4. An inventory or overview of the potential hazards
5. The risk assessment method – the means of identifying the unwanted events
6. The reason for selection of the risk assessment method
7. The risk analysis method – the means of calculating and examining the level of risk
8. The reason for the selection of the risk analysis method
9. The qualification of the consultancy to carry out the works scoped
10. The facilitator for the risk assessment with detail of qualification for the assessment
11. The suggested risk assessment team membership
12. The time required for preparation, the exercise and the write up
13. The suggested location / venue for the exercise
14. The means of providing the risk assessment results
15. Costs and dates for the project

7.1.3 Report format

Report Format Checklist

A good Report should include the following:

Executive Summary

- Introduction
- Context strategic, corporate and risk management
- Issues / reasons for review

Objective

Method (and reason for choice of method)

- Team (names, positions and related experience)
- Hazard inventory table
- External threats
- Core assumptions
- System description, boundaries and documentation
- Risk identification technique and reason for choice
- Risk analysis method and reason for choice

Results (tables, charts, etc.)

- Priority risks by magnitude of risk and consequence
- Priority existing controls and performance indicators
- Priority new controls and performance indicators

Recommended Action (the Action Plan information)

7.1.4 Review Checklist

Risk Assessment Review Checklist¹¹

A review of a risk assessment should consider the following issues

1. Is the reason for the review defined?
2. Are the objectives of the review stated?
3. Is there a description of the system being assessed?
4. Are the boundaries clearly and unambiguously defined?
5. Is the documentation provided sufficient to understand the scope and function of the system?
6. Is there a summary of the strategic, corporate and risk management context?
7. Are the participants identified together with their organisational roles and experience related to the matter under consideration?
8. Is the range of experience/expertise of the team appropriate?
9. Is the facilitator identified together with related experience?
10. Is the facilitator appropriate?
11. Is the method of identifying the risks clearly identified?
12. Is the reason for the choice of methodology explained?
13. Is the method of assessing likelihood and consequence of the risks identified?
14. Is the reason for the choice of methodology explained?

¹¹Adapted from MDG1014

15. Is there a hazard inventory table?
16. Is there a listing of external threats?
17. Are all the core assumptions identified?
18. How was the acceptability of the risks determined?
19. Is the determination of the acceptability of the risks justifiable?
20. Are all the risks prioritised by risk magnitude and consequence magnitude?
21. Was the hazard identification process comprehensive and systematic?
22. Has the approach to each part of the study been consistent?
23. Have all the existing controls and performance indicators been identified and their function determined accurately?
24. Have all potential new controls been identified, adequately assessed and assigned performance indicators if adopted?
25. Is there a recommended action list giving actions, responsibilities and timelines for completion?
26. Is there a review process to ensure the assessment is consistent with others completed at the same facility/business?

APPENDIX A. Definitions (from AS4360 unless otherwise stated)

Acceptable risk

The residual risk remaining after controls have been applied to associated hazards that have been identified, quantified to the maximum extent practicable, analysed, communicated to the proper level of management and accepted after proper evaluation (SSDC: System Safety Development Center Glossary of SSDC Terms and Acronyms, SSDVC-28 (DOE))¹.

Assumed risk

A specific, analysed residual risk accepted at an appropriate level of management. Ideally, the risk has had analysis of alternatives for increasing control and evaluation of significance of consequences (SSDC: System Safety Development Center Glossary of SSDC Terms and Acronyms, SSDVC-28 (DOE))¹.

Barrier

Anything used to control, prevent, or impede energy flows. Types of barriers include physical, equipment design, warning devices, procedures and work processes, knowledge and skills, and supervision. Barriers may be control or safety barriers or act as both (SSDC: System Safety Development Center Glossary of SSDC Terms and Acronyms, SSDVC-28 (DOE))¹.

Consequence

The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Cost

Of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, political and intangible losses.

Criticality

The categorisation of a hardware item by the worst case potential direct effect of failure of that item. In assigning hardware criticality, the availability of redundancy modes of operation is considered. Assignment of functional criticality, however, assumes the loss of all redundant hardware elements (NSTS 22254: National Space Transportation System, Methodology for Conduct of NSTS Hazard Analyses (NASA))¹.

Event

¹ Stephenson, Joe 1991. System Safety 2000: a practical guide for planning, managing, and conducting system safety programs. New York: John Wiley & Sons.

An incident or situation, which occurs in a particular place during a particular interval of time.

Event tree analysis

A technique which describes the possible range and sequence of the outcomes which may arise from an initiating event.

Failure mode and effects analysis (FMEA)

A procedure by which potential failure modes in a technical system are analysed. An FMEA can be extended to perform what is called failure modes, effects and criticality analysis (FMECA). In a FMECA, each failure mode identified is ranked according to the combined influence of its likelihood of occurrence and the severity of its consequences. A FMEA basically asks the questions: how could each component conceivably fail? What might cause these modes of failure? What would be the effect if these failures did occur? How is each failure mode detected?

Fault tree analysis

A systems engineering method for representing the logical combinations of various system states and possible causes which can contribute to a specified event (called the top event).

Formal Safety Assessment (FSA)²

A formal investigation of the nature, likelihood and impact of (FSA) potential major accident events and the means to prevent or minimise their occurrence or consequences to as low as reasonably practicable. Within the context of the safety case the term “formal safety assessment” may also refer to the reporting of facility-specific studies conducted by the operator that provide reasoned arguments and judgements about the findings of the formal investigation.

Frequency

A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.

Hazard and Operability Study³

Is a structured brainstorming approach to identifying both hazards and operability problems. The study, carried out by a multidisciplinary team, is applicable to any situation which can broadly be described as a process. The objective is to complete a comprehensive and systematic study of a facility, section by section, evaluating the significance and consequence of deviations from the design intent. It is a brainstorming process, using guidewords, and based, usually, on flow, process and instrumentation diagrams. The process can be applied to computer control systems, SOPs, batch processes, emergency response programmes etc using appropriate guidewords and team members.

Hazard

A source of potential harm or a situation with a potential to cause loss, an uncontrolled exchange of energy.

Independent Protection Layer (IPL)

² Department of Industry, Science and Resources, Petroleum and Electricity Division – Guidelines for the Preparation and Submission of Facility Safety Cases 2nd Edition

³ Adapted from ICI Engineering HAZOP Course Notes 1985

An IPL is a device, system or action that is capable of preventing a scenario from proceeding to the unwanted consequence and is independent of the initiating event or any other layer of protection associated with the scenario.

Inherent Safety

A concept best summarised by Trevor Kletz¹², who pioneered the term, as follows: “What you don’t have can’t leak”. The idea is to design and construct the mine, facility, building etc that is inherently safe, rather than designing/building something that needs substantial safety systems (hardware and software) in order to be made safe. Simplicity is part of inherent safety – “what you don’t fit costs nothing and needs no maintenance

Job Safety Analysis (JSA)

A JSA is a task oriented risk assessment which can be applied by a work team prior to undertaking a potentially hazardous activity. Generally the technique is applied on site for routine activities as a precursor to a safe working procedure. It uses job observation and experience as the basis for identifying hazards and controls to be used. It is a primitive, but helpful, qualitative analysis.

Layer of Protection (LOPA)

LOPA is a simplified method of risk assessment that provides the middle ground between a qualitative hazard analysis and a traditional quantitative analysis. From an identified accident scenario and using simplifying rules to evaluate initiating event frequency, independent layers of protection and consequences to provide an order of magnitude estimate of risk⁴.

Likelihood

Used as a qualitative description of probability or frequency.

Loss

Any negative consequence, financial or otherwise.

Monitor

To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Organisation

A company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

Probability

The likelihood of a specific event or, outcome measured by the ratio of specific events or outcomes to the number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicating an impossible event or outcome and 1 indicating an event or outcome that is certain.

Residual risk

The remaining level of risk after risk treatment measures have been taken.

¹² T A Kletz, “Cheaper Safer Plants – Notes on Inherently Safer and Simpler Plants” IChemE

⁴ Layer of Protection Analysis, Centre for Chemical Process Safety ISBN 0 8169 0811 7

Risk

The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

Risk acceptance

An informed decision to accept the consequences and the likelihood of a particular risk.

Risk analysis

A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk assessment

The overall process of risk analysis and risk evaluation.

Risk avoidance

An informed decision not to become involved in a risk situation.

Risk- benefit analysis

Evaluation of risks and benefits of some activity or agent usually based on economic consideration⁵.

Risk identification

The process of determining what can happen, why and how.

Risk management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk management process

The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Risk reduction

A selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.

Risk treatment

Selection and implementation of appropriate options for dealing with risk.

⁵ Molak, Vlasta 1997. Fundamentals of risk analysis and risk management. Lewis publishers.

APPENDIX B. Templates for Risk Assessment Tools

The following templates are provided as a guideline to the needs of each type of study considered. The templates must be treated as a guideline only and varied as required to satisfy the specific risk assessment being addressed.

- Hazard and Operability Study (HAZOP)
- Failure Modes and Effect Analysis (FMEA)
- Failure Modes, Effects and Criticality Analysis (FMECA)
- Human Error Analysis (HEA)
- What If...? Analysis
- Workplace Risk Assessment and Control (WRAC)
- Preliminary Hazard Analysis (PHA)
- Level of Protection Analysis (LOPA)

Hazard and Operability Study (HAZOP) Template ¹

Project:				Node:			Page:	
Node Description:						Date:		
						Drg No:		
Team leader:		Team Members:				Minutes By:		Pages:
Guideword	Possible Cause(s)	Consequence	Safeguard (existing)	Rec#	Recommendations	Accountability	Action	Action Ref#

¹ Adapted from ICI Australia Engineering Hazard Study Course Notes

Failure Modes and Effects Analysis (FMEA) Template²

Project No;		Component:			Page:	
Component Description:					Date:	
					Drg No:	
Team Leader:		Team Members:			Minutes by:	Pages:
No	Failure Mode	Detection Method	Equipment Affected		Safety Systems Response	Comments
			Identification	Effects		

² Adapted from ICI Australia Engineering Hazard Study Course Notes

Failure Modes, Effects and Criticality Analysis (FMECA) Template³

Project No:			Component:				Page No:		
Drg Nos:			Team Leader:				Date:		
			Team Members:				Reference No:		
			Minutes:						
No	Component Description	Failure Mode	Effects on			Probability	Consequence	Criticality	Control
			Other item	System	Safety				

³ Adapted from AIChE CCPS Guidelines for Hazard Evaluation Procedures

Human Error Analysis (HEA) Template⁴

Project No:			Key Task:				Page: of		
Task Description:							Date:		
Team leader:		Team Members:				Minutes By:		SOP References:	
No	Sub-task or element	Potential human error	Hazard exposed to/possible outcome	Possible root cause(s) of error	Possible contributory factors	Existing mitigating factors	Additional safeguards proposed	Agreed action	Accountability

⁴ Adapted from NSW Department of Mineral Resources MDG1010

What If...? Template⁵

Project No:			Section:			Page No:
Description and Purpose:					Reference Documents:	Date:
Team Leader:		Team Members:			Minutes By:	Drg No:
No:	What If...?	Concern	Safeguards	Additional Safeguards proposed	Action required	Accountable

⁵ Adapted from ICI Australia Engineering Hazard Study Course Notes

Workplace Risk Assessment and Control (WRAC) Template⁶

Project No:				Project Title:				Page: of	
Operation Description:					Documents:			Date:	
Team Leader:					Team Members:			SOPs	
Minutes By:									
	A	B	C	D	E	F	G		
No	Step in Operation	Potential Incident/Accident	Probability	Consequence	Risk Rank	Current Controls	Recommended Controls	Agreed Action	Accountability

⁶ Adapted from The CCH/ALARA Workplace Risk Assessment and Control Manual

Preliminary Hazard Analysis (PHA) Template⁷

Project:				Section:		Page:
Description of Scope Boundaries				Drawing Nos:		Date:
				Design Status:		
Team leader:			Team members:			Minutes By:
No	Hazard	Cause	Major Effect	Hazard Category	Corrective Action/Preventive measure	Accountability

⁷ Adapted from AIChE CCPS Guidelines for Hazard Evaluation Procedures

General Format of LOPA Template⁸

Project No:		Section:						Date:	
System Description:				Reference Documents:				Page:	
Team Leader:		Team Members:				Minutes by:			
Consequence and Severity	Initiating Event (Cause)	Initiating Event Challenge Frequency /yr	Preventive Independent Protection Layers Probability of Failure on Demand (PFD)				Mitigation Independent Protection Layers (PFD)	Mitigated Consequence Frequency /yr	
			Process Design	BPCS (DCS)	Operator Response to Alarms	SIF (PLC Relay)			

⁸ Adapted from A M Dowell and D C Hendershot, Simplified Risk Analysis- Layer of Protection Analysis (LOPA) AIChE 2002 National Meeting Paper 281a

Hazard/Risk Register Template⁹

Project No:				Section of Facility:				Date:		Page:				
Description of Scenario:								Team Leader:						
Reference Documents:								Team Members:						
								Minutes By:						
Item No	Initiating Event	Description of Potential Consequences (including magnitude and Effects)					Existing Control Measures					Description of Likelihood of Potential Effects (On/off site) and Likelihood Rating	Risk Ranking	Actions
		Type And Magnitude	Description of Potential Effects(on site and off) and consequence Rating				Description	Critical Control?	SMS Ref	Performance Std NO	COP Data Sheet			
			People	Biophysical Environment	Property	Economic Impact								

⁹ Adapted from MIHAP No 3 Planning NSW Hazard Identification, Risk Assessment and Risk Control

APPENDIX C. Informal Risk Awareness Tool

A Buddy System

The Buddy System is a technique of observing people doing work and helping people anticipate what could go wrong so they can prevent injury.

When?

Anytime work is going on or people are moving about.

Where?

Plants, offices, roads, laboratories, workshops, stores, stairs etc.

Who?

- Equipment technicians
- Laboratory technicians
- Contractors
- Leaders
- Environmental Advisers
- Visitors
- Fitters
- Operators

How Will It Affect Me?

- People will ask you:
 - What work are you doing?
 - What could go wrong?
 - How could it be made safer?
- You will be trained to help others prevent injury as part of the team effort.

The Buddy system will reduce the chance of you becoming injured.

Why? People's actions can prevent injury.

What? Helping people to prevent injury.

Where? Everywhere.

When? Anytime.

Who? Everybody.

How? Person to person.

B Stop! Take 5

1 Think Through the Task

“Have a clear plan in mind.”

- Understand
- Right information
- Procedure to follow
- Right tools and equipment
- Right permits
- People or systems affected
- Safe access

- Nearby equipment
- What could go wrong
- Alternative methods

2 Spot the Hazards

Look Close Look Wide Look Above

For each step, consider:

- Can the person be struck by anything?
- Can the person strike against anything?
- Can the person be caught in, or between anything?
- Can the person strain or overexert?
- Can the person slip or trip on anything?
- Can the person fall in any way?
- Can the person come in contact with or be exposed to any injurious conditions such as chemicals, heat, fumes or noise?
- Can the person injure a fellow worker?
- Can damage to equipment occur?
- Can pollution of the environment occur?

3 Assess the Risks

Is it probable?

- Improbable?
- Frequent?
- Occasional?
- Remote?

What are the consequences?

- Injury?
- Environmental Impact?
- Property damage?
- Business interruption?

4 Make the Changes Control and Communicate

- Remove the hazard
- Isolate the hazard
- Barricade the hazard
- People behaviour
- Systems

5 Do the Job Safely

APPENDIX D. Acquisition Checklist

Safety Health And Environment

1. Details of Sites, Organisation and Management

- geography and geology of sites, proximity and nature of nearby communities, industries, waterways and underground services
- history and use of sites
- product range and key developmental products
- brief description of plant and processes
- general site organisation and responsibilities for safety, health and environment management, including product, fire and transport safety
- electrical safety
- potential process safety management problems with current operations on the sites, such as major hazard chemicals or processes which may give rise to fire, explosion loss of containment, toxic gas emissions
- geotechnical structural stability
- fire prevention and the protection of people and assets
- site security provisions and procedures
- brief details of procedures for treatment of gaseous, liquid and solid effluent, waste disposal, provision for effluent containment in the event of spillage, fire water and clean up operations
- potential environmental problems with current activities or previous activities on the sites which might be associated with contamination of soil or ground water, etc, including warehouses or disposal sites away from the main site, which could give rise to legal liabilities
- condition of drains and effluent treatment equipment
- potential problems with noise
- brief details of health and hygiene programmes, assessment of new materials and arrangements for risk assessment of products
- brief details of major occupational health risks, current and historical:
 - noise
 - manual handling strains
 - carcinogenic and toxic chemicals
 - asbestos
 - sensitisers
 - radioactive sources
 - other(eg heat, light, non ionising radiation)
- brief details of on-site and off-site emergency and crisis management plans
- check potential distribution problems, such as significant movement of hazardous materials

2. Legal

- compliance with local requirements in safety, health and environment legislation
- compliance with local requirements for hazardous substances assessment, notification and communication (labels, data sheets, etc), transport safety
- check difficulties with or significant infringements of regulatory requirements, licences, permits to manufacture or to discharge effluent
- check relations with regulatory authorities
- check relations with local community, media, pressure groups
- check personal injury claims, employer's liability and third party claims: product liability claims, private property damage claims

- check insurers, insurance cover for employees, plant and liabilities for site and off-site warehouses, waste disposal sites or formerly owned sites

3. Technical Performance

- corporate performance on SH&E
- details of injury and unusual incident statistics, for safety, health and environment, over say a five year period
- arrangements for injury and incident investigation and procedures for taking action
- details of hazardous materials or processes with inventories, copies of MSDSs
- arrangements for assessing safety of plant and processes in terms of fire, explosion and loss of containment
- procedures for systems of work
- arrangements for hazard and risk management, copies of studies
- procedures for control of change, copies of forms and examples
- arrangements for monitoring and auditing plant and process safety, health and environment procedures and all safe systems of work, with copies of recent monitoring and audit reports
- performance over previous five year period against regulatory requirements for health and hygiene monitoring against occupational exposure standards
- details of occupational illness over last five years
- arrangements for investigating suspected work related health effects
- arrangements for selection, issue and controlling use of personal protective equipment
- arrangement for selection, installation and calibration of noise and atmospheric measuring equipment
- arrangements for routine health surveillance for specific circumstances, eg pre-employment, return to work, drivers, food handlers, noise exposed workers and specific substance exposures
- arrangements for workplace health hazard assessments, documentation and communication
- arrangements for first aid provision
- procedures for safe operation of process plant and equipment
- arrangements for raw materials assessments, documentation and communication
- arrangements for product safety assessments, documentation, label and safety data sheets and supply to user
- arrangements for product registration
- arrangements for packaging, transport and distribution
- performance over five years against environmental requirements related to local legislation
- arrangements for monitoring and recording gaseous emissions, liquid effluent treatment and disposal of solid waste or hazardous waste on or off site
- records of losses of containment contained within the site and those affecting the public outside the site, legal action taken by the regulatory authorities
- assessment of the state of the operating plant and equipment and also the effluent treatment facilities, in terms of age, technology, maintenance standards, suitability for duty and operating effectiveness, copies of preventative maintenance schedules and equipment histories
- selection and control of contractors
- equipment for handling of materials
- procedures for recording potential and known contamination of soil and ground-water

4. Management of Safety, Health and Environment

- existing management system incorporating a safety management system
- system comprehensive and integrated wrs to control measures, used in practice and regularly audited for best practice
- management commitment to risk management processes
- effective safety, health and environment policies with clearly defined responsibilities
- safety, health and environment improvement programmes with resources and capital allocated
- plans for the control of all emergencies, carrying out of emergency exercises
- induction and ongoing SH&E training programme
- housekeeping standards

5. Engineering Issues

- current SH&E policy
- SH&E organisation
- Training/training records
- control of change system
- control of visitors
- road vehicles on site
- safe operation of fork lift trucks
- safe operation of mobile equipment
- permit to work procedures include
 - isolation of plant from hazardous materials
 - isolation of plant from hazardous energy sources
 - entry into confined spaces
 - excavations and break ins
 - hot work
 - work on roofs
 - lone and isolated workers
 - control of ionising radiation
- industrial explosives control
- decontamination of equipment
- control of contractors
- design process for new plant and equipment
- audit of operations and engineering
 - management systems
 - occupational health
 - engineering
 - transport
 - environment
 - fire risk
- storage of hazardous materials to standard
- inspection system for all storages
- fire risk management plan
- emergency evacuation plan
- emergency response procedure
- hazardous material inventory
- fire equipment test program
- plant dossier
- effective signage in high risk areas
- site containment of fire water and spillages
- all documents under document control

- hazard assessment studies covering existing operations
- hazard studies covering changes to existing operations
- hazard studies covering all new operations
- hazard evaluations of all major activities
- all software under change control
- effective risk management programme in place
- managed maintenance system in place
- programmed maintenance system in place
- documentation on all items of equipment including history
- hazardous area classification carried out and documented
- electrical equipment appropriate to the area classification
- records of all equipment in hazardous areas
- all pressure systems registered and inspected to required schedule
- files for each pressure system
- reports for all inspections on file
- safety devices tested and recorded
- all lifting equipment registered and inspected, records kept
- all equipment marked with the SWL and unique identifier
- system for hire of lifting equipment
- system for issue, return and discard of lifting equipment
- all protective systems assessed for criticality and designed accordingly
- all protective systems have file on design intent and settings for all critical systems
- record of proof test of all critical systems
- evidence of adequate management of critical protective systems
- records of inspections carried out to ensure structural integrity is maintained
- design and condition of structures indicative of effective management system
- procedures for control, operation and maintenance of the LUV and HV distribution systems
- procedures for electrical isolation prior to working on machines, adjacent to electrical equipment, or live testing
- procedures for identification, registration and examination for equipment supplied via plug and socket
- procedure for registration and examination of equipment for use in hazardous areas
- records of all electrical equipment and history
- audits of electrical equipment against the applicable codes
- appropriate measures taken against static electricity and lightning
- design and maintenance of equipment provides evidence of an effective management system
- change control procedures for all programmable electronic systems
- documentation on design intent, proof testing and service failures of all safety related programmable electronic systems
- all machinery critical to process or safety on regular schedule of inspections including condition monitoring
- all protective devices required for the machines in place and operational

APPENDIX E. HAZOP Audit Checklist

1. Introduction

This document is a checklist for auditing the output of a HAZOP study to ensure that the integrity of the process has been maintained

2. Checklist

Planning Phase

Was the type of HAZOP methodology to be used properly identified (eg batch, continuous, etc)?

At what stage of the project was the HAZOP carried out?

Who initiated the HAZOP study?

Was there any checking procedure to ensure that all the necessary HAZOPs are done?

Did the HAZOP start only when all the data was available?

Did the timing of the HAZOP and the project allow the incorporation of the HAZOP findings?

Did the scope of the HAZOP take into account the potential interactions between new and existing plant?

Initial Study Inputs

Were the project objectives clear?

Was the process description provided?

Was the operating philosophy/design basis clearly identified?

Was the safeguarding philosophy clearly set?

Was there a readily referenced set of environmental and ergonomic constraints?

Were the layouts and hazardous area drawings available?

Were the draft equipment specifications readily referenced?

Were outline start up and shut down procedures known?

Were the outputs of previous hazard assessments made available for review by the team?

Team Composition and Size

Was the size of the HAZOP team appropriate to the study?

Did the team contain the necessary expertise?

- independent leader
- project engineer
- process engineer
- operations representative(s)
- maintenance representative
- any other

Did the team facilitator have the appropriate training and experience?

Was the training and experience of the other team members appropriate for the study?

Did the leader have the strong support of the project and the operations management?

Authority and Commitment Level

Did the team members have the authority to take decisions which would be accepted by the groups they represented?

Were the operations members involved in drawing up the design basis?

Will the operations members be involved in operating the facility?

Did the project team members have the authority to agree actions when appropriate?

Was there any specialist input that was considered important but either not requested or unavailable for the HAZOP?
Were the authority levels defined?

HAZOP Process and Documentation

Were all lines , vessels and auxiliary units studied?
Was the sequence of lines /vessels planned prior to each major section of the study and followed logically?
Was a list of all P&IDs to be studied drawn up and methodically worked through?
How was the HAZOP process controlled and documented?

- P&IDs marked up; colour coded?
- line index tag system?

Was there a master set of P&IDs used for mark up?
Was there any unnecessary duplication of identical lines?
Were any lines incorrectly assumed to be identical?
Were suitable break points chosen between lines to permit effective analysis?
Were all guide words/deviations considered?

- were they discussed and closed out rigorously?
- were minutes recorded for all guide words/deviations or by exception only?

Were consequences pursued far enough?

- sample and confirm some of the “ no consequences “ results to check whether sufficient information is provided

Were solutions predominantly hardware or software?

- was the need for procedures recognised?

Were the operator needs recognised?

- information(pre alarms, process data etc)
- facilities for rectification of deviations(restart after trips etc)
- access(local/remote trip resets , controls , etc)

Were solutions consistent with the operating philosophy (including the alarm/trip/control philosophy)?
Were the records clear?

- concerns identified?
- consequences and plant reactions listed?
- were the process components identified by equipment item numbers?
- were the actions fully defined as stand alone items?

Were the main findings summarised at a generic level for management review?
Were the HAZOP sessions carried out as marathon sessions or in 4 to 6 hour grabs?
Were the main findings presented to plant project management for early review?

Follow Up

Who is responsible for follow up on action items?
Has the follow up been clearly recorded?
How is the follow up monitored-at what level and at what frequency?
Were the HAZOP action items prioritised ? If so on what basis?
Were hazards involving risk based decisions singled out for special attention?
Was any schedule set for the close out of action items?
Was the follow up closed out at an appropriate time for the project?

Quality of the Follow Up

Does each of the action responses address the prime concerns of the HAZOP recommendations?
Were the actions consistent with the intent of the original design basis operating and

maintenance philosophies?

Was the project change control procedure applied to major actions arising out of the HAZOP?

If any significant changes resulted from the HAZOP has another full or partial HAZOP been performed on the modified design?

Was there a system for HAZOP action status update?

General Review

Was an early phase hazard assessment conducted to give the basis for the risk assessment strategy for the whole project?

Has the performance of the HAZOP study and follow up received the broad support of all functional groups?

- project design team
- operations
- maintenance
- risk management
- any other

APPENDIX F. Health Risk Assessment Outline

Although the information on risk assessment in the body of NMISHRAG applies equally to health issues as well as to safety issues, too often there has been a trend to, either ignoring health because of the immediacy of safety issues, or treating health issues rather superficially until there is an issue. There is clearly a need to ensure adequate focus is given to health issues and the long and short term consequences that may arise if they are not managed adequately. What follows, in the first section, is an outline of a health risk assessment process. It is clearly following the same model as the safety risk assessment processes but references health only. In the second section is a tool for assessing chemical usage provided by the HSE in the UK. It is available as an interactive tool on the given website.

In addition to showing the process, the notes identify a wide range of potential health hazards that may occur in a minerals environment and may need addressing at the site or location under consideration.

As with a number of hazards, specialist knowledge is often required to obtain data, identify consequences and to develop strategies for managing the health hazard. An appropriately qualified, experienced person should be a part of the team addressing a health risk assessment.

1 Health Risk Assessment

1.0 Hazard Identification

The hazards existing in each work area must be defined and a hazard inventory that includes all the chemical, physical, biological and ergonomic hazards compiled (see Attachment 1 for a possible format). The inventory should include materials of construction, welding rods, metals and welding processes, insulation, refractory, paints and coatings, glues, cleaning agents, process streams, laboratory chemicals, lubricants, fuels, wastes, etc.

Hazard identification should be conducted through:

- An inventory of materials/chemicals used and a review of MSDSs;
- An occupational health survey using a simple self completed questionnaire distributed to a sample of mine personnel covering all levels of the workforce and management.
- A review of the plant process flow diagrams;
- A walk-through survey and discussions with plant personnel, looking at the plant, its processes, equipment, materials use, physical environment, products / by-products, effluents, etc;
- Consideration of the range of tasks, both routine and occasional in the plant;
- A study of any history of disease or illness from medical records, respecting confidentiality requirements;
- A review of relevant legal standards;
- A review of documented specialist advice (eg. from trade associations, standards or professional institutes) or information from similar types of operations;
- Review of any occupational hygiene or health monitoring data, respecting confidentiality requirements.

A health effect rating for each hazard must be determined. Suggested categories are given below; it is also a convenient check list for health hazards that may be present. It is not exhaustive and should be reviewed for each specific assessment.

2.0 Health Effect Rating

2.1 Life threatening health effects or disabling illness

This category should include carcinogens and reproductive toxicants (known and suspected)

In the former category are the following (not exhaustive)

Arsenic Asbestos Benzene
Beryllium/compounds Cadmium/compounds Ceramic fibres
Refractory fibres Chromium VI /compounds Coal tars/pitches
Soot Diesel Exhaust Particulates Ionising Radiation
Nickel/compounds Oil mist, mineral Radon/decay products
Sulphuric acid mist Silica/respirable crystalline Talc with asbestos form fibres
Tar/pitch/bitumen Mineral oil/anthracene UV radiation
Uranium/compounds Wood dust

In the latter category (not exhaustive)

Ionising radiation numerous organic solvents toxic metals eg lead, mercury
Biological agents

Irreversible health effects of concern

This category should include progressive chronic conditions with a known cause, these may include:

Noise induced hearing loss Dusts Fume
Occupational Asthma Skin diseases Other agents

It would also include acute/short term high risk effects associated with substances such as:

Hydrogen Cyanide Carbon Monoxide Hydrogen Sulphide
Ammonia

Severe reversible health effects of concern

Acute /short term effects related to:

Sulphur dioxide Solvents Ozone
Phosgene Mineral acids Eye, nose, throat elevated irritants

Other Items

Musculo-skeletal effects
Nervous system effects
Potroom asthma
Infectious diseases

Reversible health effects of concern

Might include such conditions as:

- Extreme temperature effect

- Travel effects
- Stress
- Sunburn
- Narcosis
- Moderate irritation of eyes, nose, throat

Reversible health effects of little concern or no known or suspected health effects

This might include conditions such as:

- Minor irritations to eyes, nose, throat
- Offensive smells
- Nuisance noises
- Minor unaccustomed muscular discomfort
- Minor unaccustomed cardiovascular discomfort
- Minor headaches

3.0 Exposure Characterisation

Exposures must be characterised for Similar Exposure Groups. A possible format is provided in Attachment 3. A job and task analysis should be conducted to determine which hazards exist within each SEG. The website <http://www.exposedata.com> may be used for determining the potential for exposure.

Where quantitative exposure data is not available, the following qualitative assessment criteria may be of use:

- *Very high or critical* (5) i.e. Frequent contact with the potential hazard at very high concentrations;
- *High* (4) i.e. Frequent contact with the potential hazard at high concentrations, or infrequent contact with the potential hazard at very high concentrations;
- *Moderate* (3) i.e. Frequent contact with the potential hazard at moderate concentrations, or infrequent contact with the potential hazard at high concentrations; or
- *Low* (2) i.e. Frequent contact with the potential hazard at low concentrations, or infrequent contact with the potential hazard at moderate concentrations.
- *Negligible* (1) i.e. Infrequent contact with the potential hazard at low concentrations;

Quantitative assessment must be conducted for SEGs where:

- Exposures could exceed, or have exceeded, an occupational exposure limit (OEL);
- Exposures have aroused complaints or adverse symptoms directly or indirectly related to chemical or physical agents in the workplace;
- Exposures are the result of a change in activities or processes that could potentially increase exposures;
- Exposures are to carcinogens, ionising radiation or crystalline silica; or
- Required by regulations.

Hazards with very low exposure potential must be documented but need not be further assessed. However, this assessment must be reviewed periodically.

4.0 Risk Assessment for Prioritising Monitoring and/or Assessing Adequacy of Controls

The following steps for risk assessment are recommended:

- Where consistent with confidentiality and anti-discrimination laws, review all the monitoring data for employee health checks, the general workplace, personal monitoring and specific operations, and their relevance with regard to toxicity (OEL, duration of exposure, individual susceptibility, etc.).
- Determine an exposure rating for each SEG for each relevant hazard. This rating must record existing control equipment and procedures; good monitoring data is critical here.
- Conduct a health risk analysis using a risk matrix (see 5.0 below) to determine relative (not absolute) risk. The matrix axes are the health effect rating (see earlier) and the exposure rating (see earlier).
- The action identification and prioritisation is then determined from the risk matrix and the hierarchy of controls.

Recommended control actions must be documented.

5.0 Health Effect and Exposure Rating Matrix

Note that a rating of 5 is considered most serious, while a rating of 1 is least.

The following figure provides an example of a health effect and exposure rating matrix; the higher the health risk, the higher the priority for action - health risk rating = health effect rating x exposure rating, indicated by four bands of risk severity, representing 'Low' (L), 'Medium' (M), 'High' (H) and 'Extreme' (E) risk regions.

Health Effect Rating	5	L	M	H	E	E
	4	L	M	H	H	E
	3	L	L	M	H	H
	2	L	L	M	M	H
	1	L	L	L	M	M
		1	2	3	4	5
	Low		Exposure Rating		High	

Whether the action needed is control, information gathering, or a combination of the two depends on the extent of the potential health risk and the certainty of the exposure assessment, as indicated by the figure below.

Health Risk Rating	E	Control Needed	Control & Information Gathering Needed	Control & Information Gathering Needed
	H	Control Needed	Control & Information Gathering Needed	Control & Information Gathering Needed
	M	Control Needed	Information Gathering Needed	Control & Information Gathering Needed
	L	No Action Needed	Information Gathering Needed	Information Gathering Needed
		Certain	Uncertain	Highly Uncertain
		Uncertainty Rating		

6.0 Risk-Based Assessment for Choosing Controls

A risk-based assessment technique for choosing between different control methods, based on simplified economic evaluation tools is presented in the paper “Economic principles in occupational health and safety”, by Niven, KJM (2000) Occupational Health Review Nov/Dec pp13-18.

The approach is based on the principles of cost-effectiveness analysis and option appraisal. It involves four basic steps and is outlined below:

- Identify the range of feasible options, including doing nothing..
- Identify and measure costs and benefits. For both ‘Costs’ and ‘Benefits’, define ‘Type’ (eg. capital, revenue, workload, health, etc.), the ‘Measure’ (eg. time, dollars, reputation, etc.) and ‘When They Will Occur’ (eg. days, months, years). The measure doesn’t need to be objective; subjective identification of units of measure and their relative magnitude may be enough. For example, you can score the impact of each type of cost or benefit using a scale of 1 to 5. These scores need to be aggregated for each option, and then ranked.
- Evaluate the risk control potential for each option using the hierarchy of controls. Scores need to be aggregated then ranked.
- Assess the superiority and inferiority of each option and make a choice about the preferred option.

For the detail please refer to the paper referenced.

7.0 Risk Assessment for Choosing Controls for Chemicals with MSDS

The ‘COSHH Essentials’ risk-based methodology published by the UK HSE can provide a useful means of assessing controls required for the many chemicals brought onto site, where

there exists a material safety data sheet (MSDS). The COSHH Essentials provides a checklist of things to do for an assessment. The contact is <http://www.coshh-essentials.org.uk>. It is available as a book from HSE Books (HSG193), Sudbury, UK; COSHH Essentials; Easy steps to control chemicals. UK Health and Safety Executive (1999)

Step 1 involves the documentation of the assessment, including date of assessment, name of the chemical being assessed, its supplier, and the tasks it is used for.

Step 2 details the three factors needed to decide on a control approach:

- Health hazard - the possible health effects from exposure to the chemical. The highest harm group is selected;
- Amount in use – grams or millilitres (= small), kilograms or litres (= medium), and tonnes or cubic metres (= large), always opting for the larger amount if unsure; and
- Likelihood of exposure, expressed as dustiness for solids or volatility for liquid chemicals that can cause harm by inhalation.

Step 3 details the identification of the control approach needed to adequately reduce exposure for the chemical and task. A risk matrix is used to determine relative risk, combining hazard group (A to E), amount used and dustiness or volatility. The order of control approach is, in order of increasing potential for harm of chemical:

Good general ventilation and good work practices;
Engineering control, typically local exhaust ventilation;
Containment or enclosure; and
Special (expert advice is required).

Step 4 suggests finding more detailed control guidance, referring to a list of provided task-specific control guidance sheets.

Step 5 suggests the development of an implementation plan and its review, considering:

- Possible interaction with other chemical or task assessment control options;
- Suitability for the processes being undertaken;
- Safety and environmental hazards; and
- The requirements of local legislation.

Appendix G. Risk Assessment Tools

This Appendix provides some information on the various tools identified in the text but not described in detail. The following tools are considered:

- Hazard and Operability Study (HAZOP)
- Computer Hazard and Operability Study (CHAZOP)
- Failure Mode and Effect Analysis (FMEA)
- Preliminary Hazard Analysis (PHA)
- Job Safety/Hazard Analysis (JSA/JHA)
- Construction Hazard Assessment and Implication Review (CHAIR)
- Energy Barrier Analysis (EBA)
- Consequence Analysis
- Human Error Analysis (HEA)

HAZOP (Hazard and Operability Studies)

Hazop is a structured brainstorming approach to hazard analysis developed in the chemical and processing industry in the 1970s. It is applicable to any situation that can be broadly described as a process. As the name suggests a HAZOP is structured to identify both hazards and operability problems.

A HAZOP is usually carried out by a team of a minimum of 4 and a maximum of around 9 people each contributing different skills and experience in design, operations, maintenance and the specific process. One of the team would be a facilitator knowledgeable in the process. The team would include people empowered to take decisions and sanction the recommendations from the team.

A diagram of the process or item under consideration is displayed for the team. It is on this diagram that the structure of the exercise in hazard identification and analysis. The diagram is divided into logical, manageable sections and each part of that section is considered separately until all the sections have been covered. For each component of the part the team considers the intention of the component and then looks for possible deviations and potential causes of deviations from the design intent.

The starting point of the study is to identify the purpose, objectives and scope of the study. This would normally be established by the person responsible for the process. Examples of reasons for a study might be to:

- Check the safety of the design
- Decide whether and where to build
- Develop a list of questions to ask a supplier
- Check the operating/safety procedures
- Improve the safety of an existing facility

The next step is to identify the specific consequences that are to be considered:

- Employee safety
- Public safety
- Environmental impacts
- Loss of plant or equipment
- Loss of production
- Liability

The HAZOP Procedure is then:

- Take a full description of the process
 - The process designer outlines the purpose of the design
 - Any questions about the scope and design are answered
- Divide the process into sections
 - The designer explains in detail the purpose of the part section, the design features, operating conditions, fittings, up and down stream issues
 - Any general questions about the part section are answered
- Apply a set of guide words to identify potential deviations
 - The generic guide words are NONE, MORE OF, LESS OF, REVERSE OF, PART OF, MORE THAN, OTHER THAN, AS WELL AS, CHANGE IN. In a chemical process the guide words would be qualified with appropriate conditions applicable to the particular study. For example: temperature, flow, pressure, quantity, impurities, phase flow, concentration, reaction, composition.
- Systematically question every part to discover how deviations from the intent of the design can occur
- Identify mechanism of detection of a deviation
- Analyse deviations to determine the consequence of any events
- Identify ways to reduce risk of an unwanted event
- Overview of process
 - When all the parts of the process have been covered, additional guidewords are used to review the process as a whole: toxicity, services required, commissioning, start up, shut down, breakdown, effluent, maintenance, noise, safety equipment, fire and explosion

The HAZOP technique is highly adaptable to any process. All that is needed is imagination and the right team selection.

CHAZOP (Computer Hazard and Operability)

A logical extension of the HAZOP process is the application of the rigorous process to the computer control systems used in many process and equipment control systems. These systems present unfamiliar hazards to the more commonly understood hazards associated with plant and equipment. For example the failure modes of control systems are not entirely predictable and there is often an assumption among process designers and operators that the control system, often viewed as a black box, is more reliable than hardware items.

The process is a useful tool to improve the understanding of the micro processor based electronic control system. For safety critical systems the more rigorous, in depth approach discussed in section 5.10 should be considered.

Three aspects of the computer based control system are covered by the process of CHAZOP.

- Hardware
- Continuous Control
- Sequence Control

Hardware in this application is not the pumps valves etc of the process but comprises various electronic components such as power supplies, operator locations, computing modules and I/O conversion units. It can best be shown on a system architecture block diagram which for purposes of the systematic study can be broken down into discrete modules ie operator interface 1, operator interface 2, controller subsystem 1 etc. The guide

words raise issues including power failures, which can introduce a degree of common mode failure, spurious data on computer links and maintenance problems. Similar guide words are used to a HAZOP but clearly the deviations being looked for are different eg

Guide Word	Deviation
More of	Blocks of data/transfer frequency
Less of	Incomplete transfer/system crashes during transfer
None of	No data transfer
Other than	Mismatch due to reformat/software change/process variable change
Sooner than/later than	Questions how measurements are processed/time out/out of sequence/averaging assumptions
Corruption of	Noise, magnetic fields, radio interference, welding, lightning
What else	Maintenance, simulation, earthing, high voltage due to fault condition, supply failure-short or long term
Reverse of	Repeat earlier steps looking at reverse effects

The majority of control applications contain a significant number of **continuous control** loops. The technique used is similar to the conventional HAZOP of a process except in this case a loop is selected for study. The loop selected need not be the simple input single output loop commonly encountered but may include a number of inputs and outputs to define a complete function.

As with HAZOP the design intent of the loop selected is explained and inputs and outputs and tunable parameters are identified.

For each input/output guide words are used to consider possible aberrations

- Bad measurement
- Transmitter accuracy
- Conditioning

Analysis of tuning parameters could consider using guide words

- Correct
- Change in process Conditions

Other phases for the checks on the entire loop include

- Control philosophy
- Safety related
- Performance

Guidewords for the overall system after individual loop checks include:

- Interaction
- Order of tuning/implementation
- Training

Sequence control is used for many tasks such as start up/shut down, monitoring and batch control. These may be implemented in a number of ways using a Vendor's high level language, a standard computing language, ladder logic on a PLC or DCS or similar. The best way to show the intent of a sequence is a flow chart, possibly several for parallel operations.

The main problem with sequence control is the possibility of interaction between sequences and with continuous control or trip systems, with areas of critical timing and the possibility of continuous execution loops occurring which block access to other parts of the sequence.

The process is first to analyse the overall operation of the sequence with typical guide words:

- Files/reports/totalisers(resetting)
- What activates/deactivates the sequence
- Communications. I/O local to card

The sequence is then broken down into fairly independent modules for example start up, running, shutdown. The operation of each module is then analysed with typical guidewords:

- Is operator intervention required
- Timing. Any critical areas
- Major equipment interactions

The next stage of the review is a second pass through the module where the flow chart is broken down into small number of self contained flowchart symbols or a step. Similar guidewords to those used for the module are used but with a different focus.

Once all this is complete there is a need to go back and check for instances where the sequence flow may loop back to an earlier point as this may not have been appreciated when the initial analysis was done. In addition guide words such as:

- Testing
- How will the sequence operation be displayed to the operator
- Training

The results are presented in a similar format to a HAZOP with action lists etc.

The team involved in these studies will have available specialist knowledge on the systems being studied, but as with all such studies there is a need for the operations and maintenance representatives to be involved.

This section is based on notes from ICI Australia Engineering Pty Ltd HAZOP Course notes of various editions and a paper by Dr J Lear, Computer Hazard and Operability Studies also published in the same Course notes.

FMEA (Failure Mode and Effects Analysis)

FMEA is usually structure around components or equipment. As in HAZOP both hazards and operability issues may be identified.

FMEA asks the basic question of what is the consequence of this component failing? The component under consideration could be a complete hydraulic system and analysed at that level i.e. failure of pump, failure of hose(s), failure of individual items or it could be examined item by item of the system. The level the analysis is completed at depends on the defined consequence being looked for.

In FMEA the following questions are considered:

- How could each component conceivably fail?
- What might cause these modes of failure?
- What would be the effect of this failure if it occurred?
- How is each failure mode detected?

The table is an example of an FMEA partial worksheet for the failure modes of a valve:

Item	Component	Failure Mode	Failure Cause	Failure Effect	Failure Detection
1	Valve V 9321	Valve mechanism jammed closed	Stem bent, gland frozen	Low flow of A	Flow meter in line
		Motor which operates valve fails to start*	Cable cut, fuse blown, motor seized, controller fails	Low flow of A	Warning lights
		Motor operating valve fails to stop	Controller fails	High flow of A	Warning lights
		Valve gasket fails	Wrong gasket, gasket incorrectly installed, gasket worn out	Small leak of A	Visible
		Valve gasket fails	Wrong gasket, incorrectly installed, gasket worn out	Large leak of A	Visible, low reading on flow meter
		Valve leaks when closed	Valve seat damaged, debris in seat, motor travel incorrectly adjusted, valve incorrectly assembled	Unwanted flow of A	Visible
		Valve blade detached	Retaining pin fails, incorrect assembly of valve	Uncontrolled flow	Flow meter giving variable or no reading when flow expected

*Indicates that the motor failure modes will be analysed separately

From these results a range of intervention strategies can be developed to manage the various hazards resulting from the failure modes.

Risk Assessment PHA “Preliminary Hazard Assessment” or “Preliminary Hazard Analysis”

A PHA is a method for the identification of hazards at an early stage in the design process. The process is described in detail in the Centre for Chemical Process Safety Guidelines for Hazard Evaluation.

The early identification of hazards is of critical importance and the completion of a PHA is the first step to an understanding of the management issues that need to be in place to control the hazard appropriately. As a design is progressed and becomes firmed up, the PHA needs to be progressively updated until more detailed assessment can be carried out.

The PHA requires a range of basic information to be generated. This includes design criteria, material and equipment specifications, mining methods, geotechnical issues, financial issues and likely environmental emissions. The entities examined for hazards would be typically materials intermediates and final products, plant equipment, facilities, access, safety equipment, operating environment, operations such as maintenance.

The initial listing of hazards provides a guide to the issues that have to be addressed in the design process to ensure that the hazards are adequately managed. It also enables preliminary strategies for the management of each hazard to be initiated and the consequences of realisation of the hazard assessed. The typical output from such an assessment would be presented in a tabular format of the form as shown below:

Hazard	Cause	Major Effects	Corrective/preventive measures and strategies

Consequence Analysis (also called Cause-Consequence Analysis)

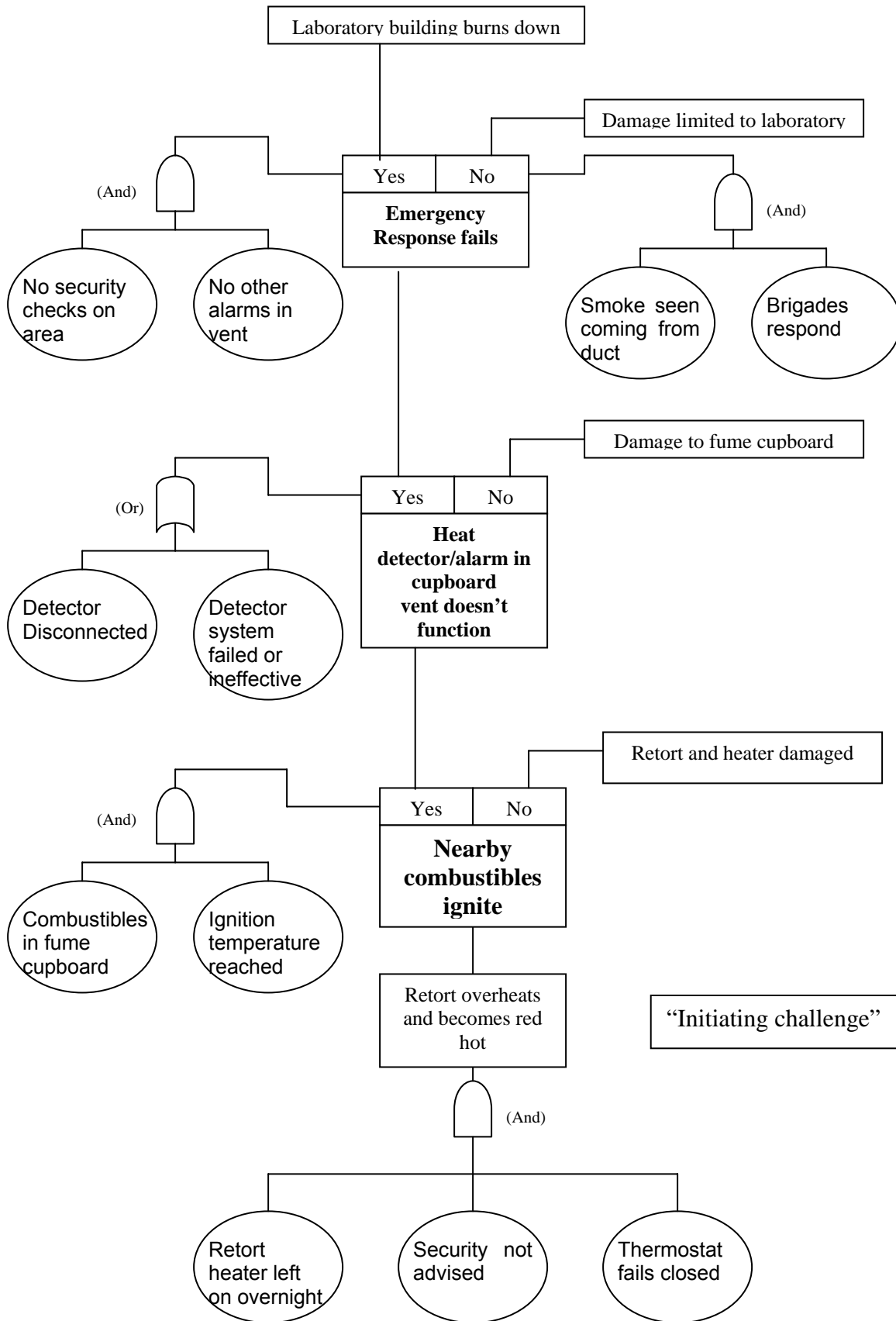
Consequence analysis is a blend of Fault Tree analysis and Event Tree analysis. When the analysis is developed, the resulting diagram displays the relationship between the incident outcome and the basic causes. The technique is most commonly used when the failure logic is rather simple since the diagram, combining fault and event trees can become quite detailed.

The analysis is a bottom up, deductive, safety system analytical technique that is applicable to physical systems, with or without human operators and to decision making/management systems. To complete an analysis, the basic knowledge required is of component failures or process upsets that could cause incidents, of safety systems or emergency procedures that can influence outcomes and of potential impacts of all these failures.

An analysis diagram for a laboratory scenario is given below. In the diagram, what is termed the initiating challenge is the rectangular box “Retort overheats”. The fault tree leading to this in this case is a simple one. It can be used to determine the probability of the Initiating Challenge. From the initiating challenge a “Branching operator” is used to explore the growth of the incident. The probabilities of the yes/no outcomes can be established by using fault trees or other analyses.

The shortcomings of the analysis are seen as the need to anticipate the operating pathways and the analysis for a single challenge only. The advantages are seen as the analysis of multiple outcomes, gradations of success/failure are distinguishable, time sequences of events are treated and end events need not be foreseen.

Consequence Analysis For "Retort Overheating"



Energy barrier Analysis (also called Energy Trace Barrier Analysis)

Energy Barrier analysis is a qualitative process that is established to identify hazards by tracing energy flow into, through and out of a system. A hazard is defined as an energy source that adversely affects an unprotected or vulnerable target

The technique identifies not only the energy source(s) but also the barriers in place to prevent the undesired release of the energy reaching the vulnerable target. Barriers can be anything from pressure container walls to steel capped shoes.

The energy flow is traced through the operation. As the energy is traced through the system, each energy transfer point must be identified. Also each physical and procedural barrier is considered to determine whether the energy still can cause undue harm.

The procedure followed is:

- Examine the system and identify all energy sources.
- For each energy source, trace its travel through the system, from beginning to end.
- Identify all vulnerable targets to the energy source along its travel path.
- Identify all barriers in the path of the energy.
- Determine if controls are adequate.

Human Error Analysis

The objective of the Human Error analysis is to identify and manage human error situations that could lead to significant hazards. The analysis can be either qualitative or quantitative, depending on the level of detail desired and the significance of the consequences. The basic steps of the analysis process are:

- Describe the system goals and functions. The system hazards are system functions that may be influenced by human error.
- List and analyse the related human operations.
- Analyse the human errors, how can the task fail because of the human input or lack? What errors can occur and can the system recover from them?
- Determine which of the errors is worthy of quantifying based on potential consequence.
- Quantify the errors and determine how they will impact on the rest of the system.
- Develop changes to the system that will eliminate or at least minimise the probability and impact of the errors.

JSA or Job Safety Analysis

A “Job Safety Analysis”¹³ is a task oriented risk assessment that can be applied by a work team prior to undertaking potentially hazardous activities.

The technique is particularly useful for developing “Safe Work Methods Statements” or Safe Work Procedures (SWP’s) where the likely level of competence of people involved in carrying out the task must be supplemented with a “set of rules” that will protect them from their competence limitations.

The JSA can be focussed on a task that has not been done previously (or for a long time) or the development of task steps prior to developing:

- ◆ A task team agreement on the way an assigned task will be carried out

¹³ Sometimes called “Job Hazard Analysis” (JHA)

- ◆ A competence enhancement program (Training).
- ◆ A task design exercise in a new or modified operating setting.
- ◆ A training needs analysis
- ◆ A Standard Operating Procedure used in a quality management system.

The process followed in a JSA is:

- ◆ Clearly identify the task steps and skill requirements
- ◆ Define the Hardware, Tooling and equipment needed to carry out the various steps in the task
- ◆ Identify the hazards (by understanding the available energies) at each task step
- ◆ Describe the necessary countermeasures, necessary to protect the people involved in the task (including bystanders) from the identified hazards

It uses original equipment manufacturer's (OEM) drawings and manuals, Material Safety Data Sheets, job observation and experience as the basis for identifying hazards and controls to be used. It is a simple but helpful technique.

In JSA's it is not wise to rank the hazards. This is because all identified hazards should be addressed with a counter-measure. The management level at which this analysis is carried out, should not provide an option to 'accept the risks associated with any identified hazard.

Sample JSA/JHA analysis

Task steps	Specialist Equipment & Tooling needed ¹⁴	Possible Hazards arising from the task step or equipment usage	Requirements to protect people from the identified Hazards

CHAIR Construction Hazard Assessment and Implication Review

A CHAIR study is a structured facilitated meeting involving designers, constructors and other key stakeholders (eg clients, specialists). To stimulate and structure the discussion, various guideword prompts are used. The process is focused on using the opportunity to make final design changes by accounting for probable construction methods. By proactively considering construction, maintenance, repair and demolition issues, the CHAIR framework not only helps reduce the number of construction industry incidents, but also assists in improving constructability and reducing the life cycle costs associated with projects.

There are three CHAIR studies nominated in the tool.

¹⁴ An optional column

CHAIR 1: which is performed at the conceptual stage of the design to provide the best opportunity to make fundamental change, even though much of the design is still to be determined.

CHAIR 2: which focuses on construction and demolition issues and is performed just prior to construction, when the full detailed design is known.

CHAIR 3: which focuses on maintenance and repair issues and is typically performed around the same time as the CHAIR 2 study.

See section 5.11 for a similar process applied as part of an overall hazard study process.

The process for CHAIR involves:

1. Assembling a CHAIR study team including all stakeholders plus an experienced leader/facilitator
2. Defining the objectives and scope of the study
3. Agreeing on a set of guidewords/prompts to assist the brainstorming process
4. Partitioning the design CHAIR 1, CHAIR 3) or construction process (CHAIR 3) into logical blocks of appropriate size.
5. For each logical block, using guidewords to assist with the identification of safety aspects/issues.
6. Discussing associated risks and determining if the safety risk can be eliminated.
7. If the safety risk cannot be eliminated, determining how it might be reduced.
8. Assessing whether the proposed risk controls (ie expected safeguards, etc) are appropriate (is the risk as low as reasonably practicable).
9. Documenting comments, actions and recommendations, as well as determining appropriately how to address any design issues still to be resolved.

For details of the application of the CHAIR process and guidewords etc see the reference ^{*} given below.

^{*} CHAIR: Safety in Design Tool; [http://www.workcover.nsw.gov.au/NR/...](http://www.workcover.nsw.gov.au/NR/) enter the title in the search function to find the document approx 100 pages

APPENDIX H. Fatigue Risk Assessment Process

Introduction

This Fatigue Risk Assessment Process is taken, with permission, from ACARP Report No C10032, "Development of a risk management tool for shiftwork in the mining industry"; Appendix A, published in November 2002 and project managed by Carmel Bofinger.

The report developed practical risk management tools that could be used by the mining industry to:

- assess health and safety risks associated with fatigue and shiftwork;
- identify and assess current and potential control measures;
- identify and assess measures for the on-going assessment of risks associated with fatigue and shiftwork.

Because of the limited amount of data available on factors affecting fatigue in mining, qualitative data gathering tools were used to investigate the impact of shiftwork on workers, including:

- (a) Health and lifestyle questionnaire - Health and lifestyle factors that can impact on how shiftwork affects workers and the impact of shiftwork on workers and their families were investigated using a questionnaire.
- (b) Sleep and alertness logs were kept by workers for 14 days and covered both sleep quantity and quality and the alertness during work periods.

Four on site risk assessments were completed based on the project model. Two additional risk assessments were completed at mines that have not participated in the data gathering parts of the project and one was completed with a contracting company. Given the limited quantitative information available on fatigue in the workplace, a qualitative risk assessment was an appropriate process that allowed the identification and ranking of the risks associated with fatigue

Based on the results of the site work, a matrix for assessing risks associated with shiftwork and fatigue was developed. This matrix was structured to allow for site specific variations. Despite differences between the mines involved in the project, there were many common factors under each heading that contributed to fatigue. This allowed the information gathered in each of the risk assessments to be combined to give an overall industry perspective.

The factors leading to fatigue in the workplace were considered under the following areas:

- (a) Work related
 - Roster design
 - Task related
 - Work environment
- (b) Non-work related.

The ordering of the risks that resulted from the risk assessments was consistent with the data obtained from the questionnaires and sleep and alertness logs.

Many of the factors that contribute to fatigue have current controls in place. In some areas these controls were assessed as insufficient to effectively control the risks. Additional control

factors that could assist in controlling the fatigue risk were identified. These were also summarised to address the common identified factors contributing to fatigue.

The report develops a fatigue risk assessment process which is described below. The process is designed to give guidance to the risk management process for individual sites by providing an industry wide perspective on the most important factors affecting fatigue and possible additional control mechanisms. Site specific issues and situations must be identified and applied to the assessment.

In addition to the fatigue risk assessment process, two other processes were developed: A guide for supervisors to assist in the identification of fatigue and a special work roster assessment matrix for non routine intensive work patterns such as shutdowns. These two processes are appendices in the original report.

The mining industry is aware of the need to manage fatigue for legislative and regulatory requirements and also for health and safety reasons for workers. The risk management process will assist mines and employees in the management of fatigue and shiftwork.

Fatigue Risk Assessment Process

At the time of the work reported here there was no suitable method available adequately to quantify fatigue in a workplace and therefore a more qualitative approach was, and still is, appropriate. The analysis technique used is based on AS/NZS 4360:1995, Risk Management.

(a) Risk Assessment

The risk assessment process is divided into:

- Risk Analysis – the systematic use of available information to determine how often specified events may occur and the magnitude of their likely consequences.
- Risk Evaluation – the process used to determine the risk management priorities by comparing the level of risk.

The following classifications are used for the risk assessment. These classifications are used for the risk assessment. These classifications are based on AS/NZS 4360:1995, Risk Management.;

CONSEQUENCES

- 1 = no fatigue resulting
- 2 = low levels of fatigue not affecting activity
- 3 = level of fatigue will cause moderate level of impairment
- 4 = high level of fatigue causing significant impairment
- 5 = very high level of fatigue causing serious impairment and / or leading to sleep

LIKELIHOOD

- A = fatigue is expected to occur in most circumstances
- B = fatigue will probably occur in most circumstances
- C = fatigue should occur at some time
- D = fatigue could occur at some time

E = fatigue may occur only in exceptional circumstances

Table H1 demonstrates the risk analysis matrix used.

Table H1

Qualitative Risk Analysis Matrix

Likelihood	Consequences				
	1	2	3	4	5
A	S	S	H	H	H
B	M	S	S	H	H
C	L	M	S	H	H
D	L	L	M	S	H
E	L	L	M	S	S

H = high risk in terms of contributing to fatigue, research and planning required at high level

S = significant risk in terms of contributing to fatigue, attention needed

M = moderate risk in terms of contributing to fatigue, responsibilities must be specified

L = low risk in terms of contributing to fatigue, manage by routine procedures

(b) Factors Causing Fatigue – Fault Tree Analysis

The assessment of the factors causing fatigue should cover the following areas:

- Work related
- Roster design factors;
- Task related factors;
- Work environment factors.

Non-Work Related

(c) Effectiveness of Current Controls

The next step involves an assessment of the current controls (both formal and informal) in place to manage fatigue. This allows identification of “residual” risk.

(d) Risk Treatment and Control Options

The potential risk treatment options need to be identified at the:

- Corporate level;
- Site level;
- Shift level;
- Individual level.

For the non-work related risks, treatment options need to be identified at the:

- Site level;
- Individual level.

Tables H2 – H5 show the summary of the risks, the ordering of the risks and possible control options for these risks.

These are provided as guidance to assist in the risk assessment process. Site specific details and issues must to be considered.

Table H2
Summary of Roster Design Factors Affecting Fatigue and Potential Controls


Roster Design Risk Factors	More Risk	Possible Control Options			
Number of consecutive night shifts		CORPORATE			
Overtime extending length of shift/unscheduled overtime		<ul style="list-style-type: none"> - Resourcing to meet site roster requirements 	SITE		
Break patterns – between shifts			<ul style="list-style-type: none"> - Policy and procedures to manage fatigue - Control of total hours worked, including overtime - Control of scheduling of hours taking into account rest and recovery needs - Identification of fatigue without disciplinary action - Resourcing and manning to allow flexibility of scheduling of tasks and breaks - Provision of training and information - Strategies for breaking pattern during shift 		
Break patterns – within shifts					
Shift length					
Time of day effects				SHIFT/WORKGROUP	
First night shift including travel before first night shift				<ul style="list-style-type: none"> - Application of site policies and procedures - Flexibility of scheduling of tasks and breaks - Culture that recognises the need to manage fatigue proactively 	INDIVIDUAL
Shift start/finish times – including time of travel					<ul style="list-style-type: none"> - Application of information from training - Reporting of fatigue
Number of consecutive day shifts					
Changes to rosters					
	Less Risk				

Table H3
Summary of Task Related Factors Affecting Fatigue and Potential Controls


Task Related Risk Factors	More Risk	Possible Control Options	
Repetitive, monotonous tasks eg haul truck driving		<p align="center">CORPORATE</p> <ul style="list-style-type: none"> - Resourcing to meet site roster requirements 	<p align="center">SITE</p> <ul style="list-style-type: none"> - Identification of physical and equipment demands for tasks - Resourcing and manning to allow flexibility of scheduling of tasks and breaks - Identification of tasks that may be "fatigue critical" - Strategies to break routines that lead to fatigue
Hard physical work – heavy workload			
Hot/humid work, confined space etc			
Vibration		<p align="center">SHIFT/WORKGROUP</p> <ul style="list-style-type: none"> - Application of site policies and procedures - Flexibility of scheduling of tasks and breaks - Job rotation - Culture that accepts the need to proactively manage fatigue 	<p align="center">INDIVIDUAL</p> <ul style="list-style-type: none"> - Application of information from training - Reporting of fatigue
Noise			
	Less Risk		

Table H4
Summary of Work Environment Factors Affecting Fatigue and Potential Controls



Work Environment Risk Factors	More Risk	Possible Control Options	
Work related stress		CORPORATE	SITE
Travel from camp/town before and after shift		<ul style="list-style-type: none"> - Resourcing to meet site roster requirements - Recognition of legislative needs 	<ul style="list-style-type: none"> - Communication strategies to assist in maintaining positive work culture - Communication strategies to encourage reporting of fatigue and proactive management - Provision of training and information including training of supervisors to recognise fatigue - Control and maintenance of the physical environment
Road conditions on site		SHIFT/WORKGROUP	INDIVIDUAL
Lighting		<ul style="list-style-type: none"> - Application of site policies and procedures - Maintenance of communication - Maintenance and reporting of the physical environment 	<ul style="list-style-type: none"> - Application of information from training - Reporting of fatigue
Lack of recognition of fatigue/lack of training			
Quality of accommodation, meals etc			
Climate conditions			
Morale	Less Risk		

Table H5
Summary of Non-Work Related Factors Affecting Fatigue and Potential Controls

Non-Work Related Risk Factors	More Risk	Possible Control Options	
Sleep disorders		SITE	INDIVIDUAL
Length of travel to and from work		<ul style="list-style-type: none"> - Provision and promotion of Employee Assistance Program - Provision and promotion of health promotion programs - Provision of training and information - Provision of transport to and from worksite - Alcohol and drug advisory training - Alcohol and drug self testing 	<ul style="list-style-type: none"> - Self management through application of information from training - Prioritisation of family and social commitments - Recognition of obligation to arrive “fit for duty”
Family commitments			
Health/diet/fitness			
Second job/non-paid work			
Alcohol use			
Drug use – legal and illegal			
Social activities			
Psychological problems			
Sleeping conditions			
General travel conditions	Less Risk		

