RM-001-02

Hazard Identification and Safety Risk Assessment Guideline

Version 1.0

Issued July 2021

Contents

1 Abbreviations and Definitions

The following list of Abbreviations and Definitions is applicable to this framework document.

ARTC	Australian Rail Track Corporation
President	OTHR Management Committee
CRN	Country Regional Network
EMS	Environmental Management System, a part of the IMS, environmental related policies, procedures, guidelines and instructions and how they are planned, integrated, implemented and approved as defined in the Environmental Protection Act, owned by the Manager SOE
Hazard	A characteristic or condition (of the network or workplace) that exists within an organisation or environment managed by that organisation
HSR	Health and Safety Representative (meeting)
IMS	Information Management System
KPI	Key Performance Indicator
KRA	Key Result Area
Near Miss	An incident type, where a failure of a system or process or unexpected or unacceptable behaviour of an individual or organisation has occurred that resulted in circumstances being created that could have resulted in a collision, strike, derailment, fall, obstruction or exceedance of specified limits or boundaries
NO	Notifiable Occurrence has the meaning as specified in the RSNL. They are incidents that require mandatory reporting by an accredited operator either immediately or not more than 72 hours after occurring. This definition covers those incidents described in Clause 57 of the RSNLNR and also covers Category A and B incidents as defined in NTC Model Rail Safety Regulations 2006, clause
ONRSR	The Office of the National Rail Safety Regulator (the Regulator), based in Adelaide with a regional office representation in NSW (NSW-based office, formerly ITSR)
RR	Principal Risk Register, the key risk document describing all foreseen risks and controls for the
QAAP	Quality Audit Assurance Program
QMS	Quality Management System, a part of the IMS, quality related policies, procedures, guidelines and instructions and how they are planned, integrated, implemented and approved and which must be certified to ISO 9001 requirements
Rail Corridor	The area bounded by and within the designated railway fence-line, or where no fence-line exists, within 15m from the nearest rail, covering both operational and non-operational rail lines
Rail Reserve	The area defined as the rail corridor, and additionally including any land identified by an act of Parliament that defines land as a rail reserve
RBAP	Risk Based Audit Program
Record	Any document or other source of information compiled, recorded or stored in written form or on film, or by an electronic process, or in any other manner or by any other means
Regulator	ONRSR, the NSW Rail Safety Regulator, a state-based office of the national ONRSR office that has jurisdiction over and is responsible for enacting the RSNL and RSNLNR as they apply in NSW

RIM	Rail Infrastructure Manager, a category of rail safety accreditation that may be held that permits the maintenance of rail infrastructure as defined in Section 4 of the RSNL
Risk	Any event that may cause harm to persons or damage to property or an organisation due to the presence of a hazard
Risk Control	A measure that exists to control the occurrence (or consequence of the occurrence) of an event that poses harm to persons, property or the environment
RMS	Roads and Maritime Services, a road manager for defined roads within NSW
RSO	Rolling Stock Operator, a category of rail safety accreditation that may be held that permits the operation of rolling stock as defined in Section 4 of the RSNL
RSNL	Rail Safety National Law (NSW), the legislation to which SJM RAIL is bound to comply for all rail safety elements relating to its obligations as a RIM
RSNLNR	Rail Safety National Law National Regulations 2012
RSW	Rail Safety Work/Worker
Safety Culture	Element 2 of the current SMS. The collective behaviours and attitudes towards the management of safety as demonstrated at the organizational, business unit and individual levels by SJM RAIL employees
SFAIRP	So Far as Is Reasonably Practicable, a measure of the level of safety management required to be demonstrated to comply with legislation
SMS	Safety Management System, a part of the IMS, rail safety and WHS related policies, procedures, guidelines and instructions and how they are planned, integrated, implemented and approved as defined in the RSNL
MT	Management Team
SPI	Safety Performance Indicator
SQE	The Safety, Quality and Environment
SQERM	Safety, Quality and Environment Risk Management, a process to structure the risk assessment processes for SQE risks
TRA	Task Risk Assessment
WHS	Workplace Health and Safety

2 Introduction

This document provides the working instructions and guidance to enable the effective undertaking of hazard identification and risk assessment. It supports the following SMS documents:

The following tools and techniques are covered in this document:

a) generic hazard identification brainstorming process

b) Preliminary Hazard Analysis (PHA)

c) System Hazard Analysis (SHA)

d) Interface Hazard Analysis (IHA)

e) Operating and Support Hazard Analysis (OSHA)

f) Failure Modes, Effects and Criticality Analysis (FMECA)

g) Fault Tree Analysis (FTA)

h) Event Tree Analysis (ETA)

i) Cost Benefit Analysis (CBA).

3 Generic brainstorming process

The purpose of the hazard identification brainstorming process is to identify hazardous events, causes, outcomes, controls, and corresponding safety risk rankings associated with an activity, change or situation. The process for conducting this is shown in Figure 1. Each process step in Figure 1 is described in more detail in the following sub-sections.

This approach is generic for all the hazard analysis approaches described in this document, but to demonstrate the application the process described is closely aligned to the process which supports the maintenance of the OTHR Engineering Risk Register.

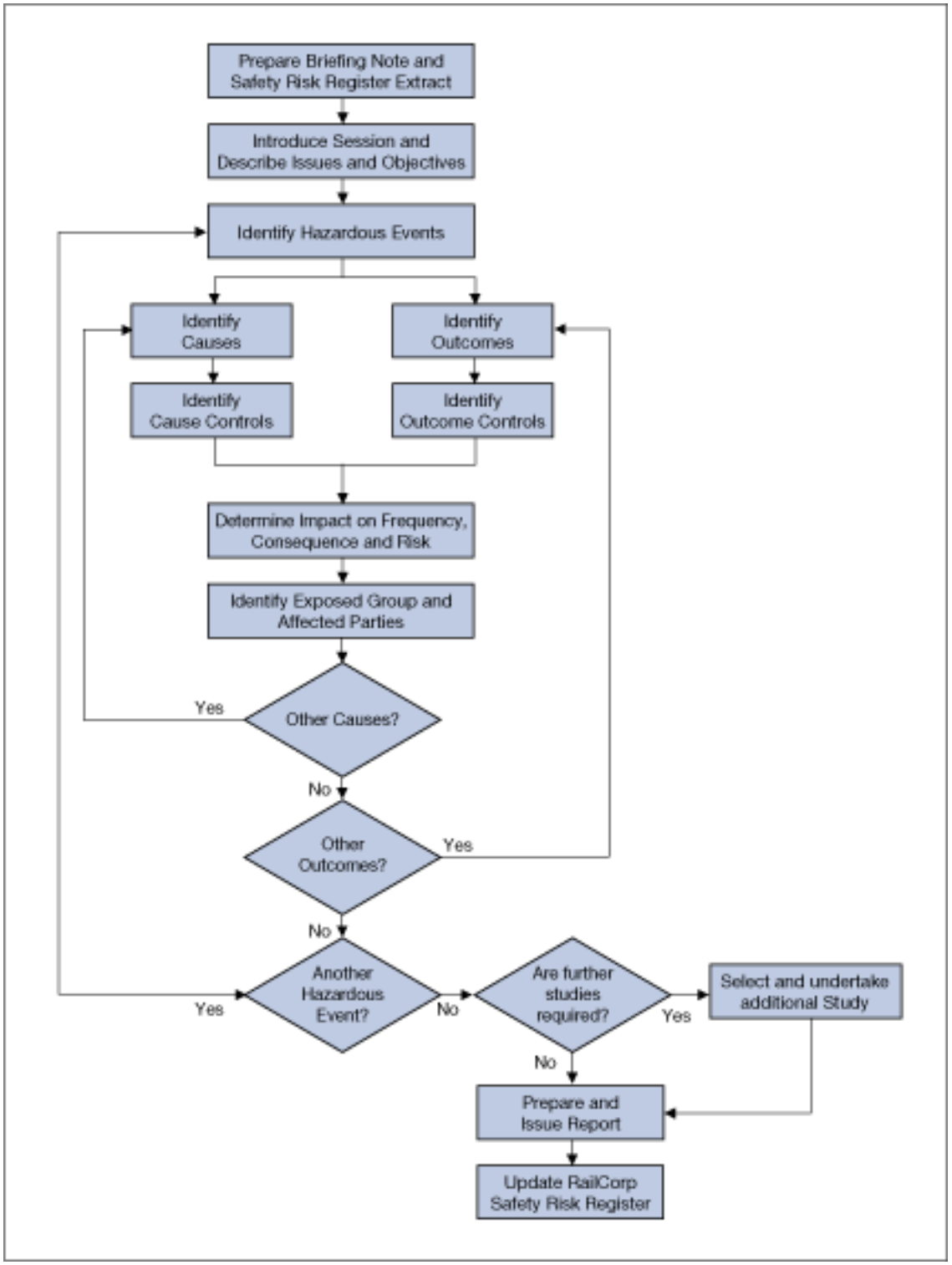

Figure 1 Hazard identification process

Ideally, records of the hazard identification sessions are created in situ, using the template provided in Appendix A. This form must be completed for all sessions to record the details identified. The completed forms should be attached as an appendix to the report produced in relation to the session.

It should be noted that even with the guidance and process described in this procedure, such sessions will be undertaken by many different people with different levels of risk understanding, interpretation, and application experience. Therefore, it is important to view the process shown in Figure 1 as general guidance.

In certain cases, the allocation of safety risk ranking is best achieved outside the sessions, allowing more focus and attention during the session to be placed on identifying causal information, outcome potential and control measure details.

3.1 Prepare briefing note and Safety Risk Register extract

The effectiveness of the session will ultimately be determined by the degree of forward planning and preparation. This will include the development and issue of a briefing note prior to undertaking the session. The briefing note should include the following details:

a) description of the issues being examined and the reason for conducting the session

b) the scope, objectives, and target outcomes from the session

c) the attendees for the session and what is required of each party; for example, if someone from train operations is being invited, it is important to summarise what is expected of them prior to, during and after the session; this should also consider the competency requirements for the session

d) an appropriate extract from the Risk Register which is used as the basis for providing focus and direction during the session. This assists with the organisational knowledge and can be used to support risk ranking (e.g. historical data helps with likelihood estimation of risk).

e) any supporting documentation, such as schematics or drawings, system diagrams, operating procedures that are reviewed or used during the sessions

f) details of who is chairing the session and who is recording the minutes

g) logistical arrangements in terms of timings, location.

3.2 Introduce session and describe issues

All sessions should start with an introduction by the facilitator where the issues being examined are described and the process and expected outcomes reiterated. Where necessary, a technical expert from within the group would be requested to provide a brief overview of the subject area to be examined. The facilitator's role is predominantly to make sure that the process is followed accordance with the safety risk management requirements, although there is also a responsibility for the facilitator to make sure that group sessions deliver realistic outcomes.

This would typically include, ensuring that the risk identification considers corporate knowledge, the recorded outcomes are a balanced summary of the considered opinion of the group, that objections/disagreements are noted and that agreed actions are realistic and within the scope of the assessment.

3.3 Identify stakeholders, context, and scope

A clearly defined scope along with an identification of the stakeholders is a key step in this process. The definition of the scope should include the following terms:

a) what is covered (and what is not)
b) where the risks are being considered
c) when the risks apply
d) who is involved?
e) what types of risk are being considered (and which are not)
f) anything else that may be used to decide which risks are to be included and which are to be excluded.

The scope should then be considered in the context under which it will be used. This would include assessing the intended purpose of the results and identifying the primary users of the information.

Once the scope and context have been determined, the stakeholders must be identified. Stakeholders are, or may be, affected by the risk or the treatments. They may be identified as individuals, or groups of people. It is important to note that when considering stakeholders, all groups or individuals who may be affected should be considered. This would include for example, consideration of vulnerable groups such as the disabled, the elderly, young children, mothers with children etc.

Identifying stakeholders at this stage in the process allows for the selection of suitable people to be involved in the risk management process. Where possible, the risk management process should be carried out with representatives of all the stakeholder groups. In the case of passengers and the public, this may involve liaison with community or lobby groups.

The following are examples of stakeholders:

a) individuals inside or outside the organisation
b) employee or union groups
c) business or commercial partners
d) financial institutions
e) customers, suppliers, contractors, and service providers
f) regulators and other government organisations
g) public interest groups or local community groups
h) society.

The preparatory work for a risk assessment would also include determination and documentation of issues such as:

a) applicable laws, regulations, standards, codes, and specifications
b) relevant competent authorities and their requirements
c) interfaces – full listing of physical, organisational and system interfaces
d) assumptions and constraints.

3.4 Identify hazardous events

The brainstorming element of the session will then progress with the identification of hazardous events relevant to the issues. This should start by reviewing relevant Safety Risk Register extracts. Caution should be exercised to make sure that the baseline structure is used, and that clear distinction is made between hazardous events, causes and outcomes and they are recorded in a consistent manner to the Safety Risk Register definitions.

3.5 Identify causes

Having identified which specific hazardous events are affected by the issues being examined, the next step in the process will involve reviewing the causal factors associated with the specific hazardous events.

The following questions should be asked of the meeting:

a) are the existing causes relevant to the accident sequence being reviewed?

b) are any existing causes eliminated because of the issues being examined?

c) are there any new causes relevant to the specific hazardous event being considered which may not already appear in the Safety Risk Register?

3.6 Identify cause control measures

Having reviewed the causal factors, the next step will involve reviewing the cause controls. As with the above causal factors, the following questions should be asked:

a) are the existing control measures relevant to the causes being considered?

b) are any controls rendered redundant because of the issues being examined?

c) are any new controls required to address either change to existing causal factors or the introduction of new causes?

3.7 Identify outcomes

In addition to examining the causal side of risk, the next step involves consideration of the impact on the potential outcomes. The following questions should be considered in relation to the Specific Hazardous Event outcomes:

a) are the existing outcomes relevant to the accident sequence being reviewed?

b) are any outcomes eliminated because of the issues being examined?

c) are any new outcomes relevant to the specific hazardous event, which may not already appear in the Safety Risk Register?

3.8 Identify outcome controls

This step should then be followed by a review of the existing outcome control measures through the following questions:

a) are the existing control measures relevant to the outcomes being considered?

b) are any controls rendered redundant because of the issues being examined?

c) are any new controls required to address either change to existing outcomes or the introduction of new outcomes?

3.9 Determine impact on frequency, consequence, and risk

Having determined the potential impact on existing causes, outcomes, and their associated controls, it will then be possible to review and determine any impact on the frequency and consequence classifications. To achieve this, reference needs to be made to the SJM Engineering Risk Matrix and the associated frequency and consequence classifications.

The consequences and likelihood of each risk are assessed using the information in the consequence and likelihood descriptors on the risk matrix. When considering likelihood, the assessment should be based upon SJM Rail activities. However, to assist estimation, consideration should be given to elsewhere in Australia (such as other railways/corporations). For example, knowledge of an event that has happened in other railways may assist in assigning likelihood to an event which has not happened to date within SJM Rail.

To score the risk, follow the steps:

a) Identify the magnitude of the credible consequence if the risk were to occur. For operational type risks, if applicable, consider the impact in terms of the safety, business and the environmental.

b) Identify the likelihood of this level of consequence occurring (this is done after considering the effectiveness of the current controls in place).

c) Using the relevant risk matrix, score the risk using the combination of likelihood and consequence.

Where it is concluded that a change is required to an existing Hazard Sequence, the new frequency, consequence, and associated risk ranking should be entered in the Residual Risk columns. Where the details recorded relate to new causes, or outcomes, then the risk ranking details should be added in the Existing Risk columns.

3.10 Identify exposed group and affected parties

The hazard identification form also requires the identification of the groups which are exposed to the hazards and the affected parties. The exposed groups include some or all the following:

a) passengers

b) public

c) employees

d) contractors.

The affected parties include, but are not limited to:

a) SJM Rail operating groups

b) others (including external and third-party users).

This information is used amongst other things to help identify who will have ultimate responsibility for the issues identified and who is required to support and authorise any subsequent actions or decisions that may be required.

3.11 Check for other causes or outcomes

Following completion of the above steps, a final check should be made to make sure that there are no further causes or outcomes that may be relevant to the hazards being examined. Where further causes or outcomes are identified, this should instigate another iteration of the previous process.

3.12 Check for another hazard

As a final check, the Chairperson asks whether any further hazards may be relevant that have not been identified through the extraction of the Specific Hazardous Events from the Safety Risk Register. To help answer this question, a set of generic guidewords can be reviewed and applied.

Typical sets of guidewords are included in Appendix B; it is beneficial to include these in the Briefing Note. These guidewords are for illustration and guidance only. Other more suitable guidewords may be applicable depending upon the nature of the issues being considered.

3.13 Determine if further studies are required

Having exhausted all potential hazards, causes and outcomes, a final review will be made of the meeting notes to determine if any more detailed risk studies are required. This will normally be determined based on the risk rankings established through the sessions.

Where any Hazard Sequence results in a risk ranking A or B, it is strongly recommended that further examination is made of the issues.

Where more detailed studies are required, these should be performed off-line from the session and the results feedback to the final report and ultimate update of the Safety Risk Register.

3.14 Prepare and issue report

All sessions will require the production of a report to record the findings, recommendations and further actions required. Pro-forma for a typical Hazard Identification and Safety Risk Assessment Report is included in Appendix C.

3.15 Update Safety Risk Register

On final issue and approval of the Hazard Identification and Safety Risk Assessment Report and any additional studies undertaken, it is important that the results are fed back to the Safety Risk Committee such that the appropriate updates can be made to the Engineering Risk Register.

4 Preliminary Hazard Analysis (PHA)

All risk studies should ideally commence with a Preliminary Hazard Analysis (PHA). This is considered the highest-level hazard identification tool and should generally be applied to examine the extent of operational and organisational factors associated with an activity or course of action. A PHA would often result in the identification of the need for further detailed analyses, e.g. through FMECA, FTA.

4.1 Purpose

The purpose of the PHA is to provide an early, high-level assessment of the possible hazards, causes and outcomes, and to initiate appropriate actions to mitigate, eliminate or control the risk potential.

4.2 Procedure

The PHA should draw upon the experience of the analyst and the system designers, operators, maintainers, and engineers as appropriate. The PHA is a qualitative analysis and can form the baseline for subsequent more detailed analyses. It is normally undertaken as a group exercise, in line with the process described in section 2 and illustrated in Figure 1.

All relevant disciplines should be represented at the PHA meeting. The relevant extract of the Safety Risk Register and appropriate high-level guidewords such as those shown in Appendix B can be used to aid identification of potential hazards within the system or activity under analysis.

4.3 Results

The PHA provides information to highlight identified hazards, causes or outcomes and to determine potential safety critical areas for further analysis. The results can then be used to perform an initial estimate of the overall risk level of the system or activity under analysis through application of the SJM Rail Engineering Risk Matrix and its associated classifications of frequency and consequence.

4.4 Documentation

The PHA results should be recorded on the standard hazard worksheets. These should then form part of a PHA Report. Appendix C provides general details of what should be contained within a typical Hazard Identification and Safety Risk Assessment Safety Report.

5 System Hazard Analysis (SHA)

A System Hazard Analysis (SHA) is conducted if there is a need to examine in detail the specific hazards in a railway system, such as rolling stock. If for example, new rolling stock is being procured, a SHA is required to look in detail at the rolling stock and the various systems that comprise the overall rolling stock system.

5.1 Purpose

The purpose of a SHA is to identify hazards, causes, outcomes and control measures which are specific to a system or its supporting sub-systems. The purpose is to further to assess the risk associated with the total system design, including software, and specifically of the sub-system interfaces, and to recommend actions necessary to eliminate identified hazards, causes or outcomes or to control their associated risk to acceptable levels.

5.2 Procedure

As with the PHA, the SHA is best performed initially as a group session in line with the general process described in section 2. As the SHA is generally used to focus on railway systems issues, a thorough knowledge of the technical performance and functionality of the systems being examined is necessary from within the selected group.

The SHA should also specifically involve establishing the following:

a) possible independent, dependent, and simultaneous hazardous events including system failures, failures of safety devices, common cause failures and events and system interactions that could create a hazard or result in an increase in risk

b) degradation in the safety of a sub-system or the total system from normal operation of another sub-system.

c) design changes that affect sub-systems

d) effects of human factors on the safety of the system

e) determination of potential contribution of hardware and software

f) determination that the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of the system nor has introduced any new hazards, causes or outcomes.

5.3 Results

The SHA results will consist of a listing of all hazards, causes and outcomes identified through the application of the SHA. It may include the following:

a) the identified causal and outcome descriptions relevant to the sub-systems, the complete system, and associated interfaces

b) details of the point at which the hazards may arise or be relevant, such as during maintenance, during degraded or emergency operations

c) the effects that the resulting hazards could have on other equipment, facilities, personnel

d) the recommended actions required to eliminate or control the hazards.

5.4 Documentation

The SHA results should be recorded on a standard worksheet. These form part of the SHA Report.

The SHA Report will generally contain more technical details than the PHA in relation to the physical and functional characteristics of the system and its components.

6 Interface Hazard Analysis

Where the operational or organisational issues identify specific interface concerns, an Interface Hazard Analysis (IHA) should be undertaken. This may be the introduction of new technology, which will impact on multiple systems, such as signalling, rolling stock, communications, or one that impacts on external parties.

The IHA specifically focuses on the definition and control of interface hazards. A area where this technique has application is in Safety Interface Agreements.

6.1 Purpose

The purpose of an IHA is to identify the hazards, causes, outcomes and control measures associated with inter-related or inter-dependent systems and/or processes.

6.2 Procedure

The IHA should be conducted in a similar manner to the previously described levels of hazard identification, for example, through the undertaking of an IHA session in the first instance, followed by more detailed analysis, as necessary. It is important that the parties involved in IHA activities provide a broad representation of the various interfacing aspects.

In the early stages of undertaking an IHA it will be necessary to define each interface at an appropriate boundary and determine responsibility. These boundaries will be selected to coincide with the logical delineation of the sub-systems.

Each interface is defined and documented in terms suitable to their function and construction. Interfaces will have several types of characteristics but, depending on the interface, will be predominantly one of the following:

a) physical, structural, and mechanical
b) technical
c) electrical
d) functional/operational
e) electromagnetic
f) human
g) environmental.

6.3 Results

The IHA results will consist of a listing of all hazards, causes and outcomes identified through the application of the process. The IHA should also clearly define responsibilities for the various control measures that may be identified and the inter-dependencies of these measures.

6.4 Documentation

The IHA will be documented using the approach described previously, for example, through recording the hazard details in the worksheet.

7 Operating and Support Hazard Analysis

An Operating and Support Hazard Analysis (OSHA) would normally be conducted where there is a perceived high degree of operator, maintainer, or procedural risk. In addition, the OSHA would particularly focus on related human factors matters, which may impact upon the overall risk.

Recognising the significance of human factors in risk management, SJM Rail has developed specific requirements and guidance on Human Factors analysis. Further information can be found in the Human Factors Management Manual.

7.1 Purpose

The purpose of an OHSA is to evaluate activities for hazards or risks introduced into the system by operational, maintenance and support procedures and to evaluate the adequacy of operational and support procedures used to eliminate, control, or minimise identified risks.

7.2 Procedure

The OHSA will normally commence by using the same approach as described in section 2. The OSHA should be used to identify and evaluate hazards resulting from the implementation of operations or tasks performed by persons with specific consideration to the following:

a) planned system configuration

b) facility interfaces

c) planned operating and maintenance environments

d) supporting tools or other equipment, including software

e) operational or task sequence

f) potential for human errors.

7.3 Results

The OSHA should conclude with a listing of identified hazards, causes, outcomes and the relevant control measures. In addition, the following should ideally be included in the results:

a) activities which occur under hazardous conditions, their time periods, and the actions required to minimise risk during these activities/time periods

b) changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks

c) requirements for safety devices and equipment, including personnel safety and life support equipment

d) warnings, cautions, and special emergency procedures (such as exit, rescue, escape, etc.), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication.

e) requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials

f) requirements for safety training and personnel certification

g) effects of non-developmental hardware and software across the interface with other system components or sub-systems

h) potentially hazardous system states under operator control.

7.4 Documentation

The OSHA result should be documented in the worksheets and in an OSHA Report.

Appendix A – Generic guidewords

Guidewords (List One)

Train accidents

- Collision between trains
- Collision between train and obstruction
- Derailments
- Train fires
- Explosions
- Dangerous goods incidents
- Rolling stock failures
- Flooding

Movement accidents

- Hit by rail vehicle
- Fall from rail vehicle
- Accidents on entering/alighting from rail vehicle
- Accidents arising from train door operation
- Hit by flying objects
- Slips and trips inside train

Non-movement accidents

- Fall down escalators/steps
- Fall from platform
- Other falls
- Electric shock
- Slips and trips
- Struck by object
- Contact with machinery
- Manual handling/over exertion
- Exposure to chemicals/dangerous substances
- Assault
- Road traffic accident
- Fires
- Explosions
- Crushed
- Burns
- Lack of oxygen

Guidewords (List Two)

Equipment/instrument malfunction

- Failure to operate
- Operates incorrectly
- Spurious operation
- No information
- Incorrect information

Operating errors and other human factors

- Changes to operating procedures
- Changes to look and layout of equipment
- Changes to workplace environment
- Changes to operator responsibilities

Maintenance, inspection, and testing

- Error at equipment handover
- Error at shift change
- Unclear responsibility for equipment
- Access authority not obtained
- Access impossible
- Incorrect labelling
- Inspection and testing inappropriate
- Inspection and testing incomplete
- Inspection and testing inadequate
- Contractors/sub-contractors
- Supervision/approval

Utility failures

- Power failure or over/under voltage
- Communications failure

External factors or influences

- Lightning
- Strong wind
- Flood
- Heat
- Humidity (wet/dry)
- Subsidence, landslide, earthquake, building collapse
- Vandalism/sabotage/civil disturbance/ terrorism
- Fire (accidental or arson)
- Vehicle impact

Loss of integrity

- Failure (component by component)

Emergency operations

- Fire alarm
- Thunder/lightning storm
- Other (unspecified emergency, no procedures)
- Failure of emergency procedures (conflicting roles)
- Fire services do not arrive

Environmental and health

- Loss of water supply
- Loss of electricity supply
- Fire
- Smoke/toxic combustion products
- Flying debris
- Electrocution
- Burns
- Impact on public