Railway Safety Regulator

# *Developing a HAZARD LOG for the Railways of South Africa*

Information Technology Guide
22 September 2021

SPRONG CONSULTING

## *Developing a HAZARD LOG for the Railways of South Africa Information Technology Guide.*

## CONTENTS

# 1 Introduction

The preliminary phase in the development of a Railway Safety Risk Model includes problem definition, data information collection and analysis, and finally hazard identification. These are listed in a Hazard Log as hazardous Events (HE). A Hazardous Event is an incident that has the potential to be the direct cause of safety harm. Estimates of frequency (likelihood or probability) and potential harm (severity of impact) will be encoded into the model.

A Hazard Log is a record keeping tool applied to tracking all hazard analysis, risk assessment and risk reduction activities for the whole-of-life of a safety-related system. It is the single source of record for all risk management activities.

The Hazard Log is a structured way of capturing and referencing safety Risk Evaluations and other information relating to a railway system, it is to be coordinated and controlled whilst maintaining an auditable record of that information. It is the principal means of tracking the status of all identified Hazards, decisions made, and actions undertaken to reduce the risk.

## 1.1 Safe Condition of a Railway System

The Safe condition of a railway system can be judged by following the logic in the decision tree in Figure ***1***.

- The first question will be whether hazards or dangers are eminent in the railway system. The Mission Critical Activities can be analysed and the Hazards that could negatively impact on these Activities, can be identified and listed.

- The following decision point is whether there are incidences that could activate the hazards and dangers and if so, whether the railway has mitigation measures or plans in place. If the answer is positive (see branch A), and frequent occurrences occur, then the railway system is considered to be a "Reactive railway system", that reacts to occurrences. An example is a railway system that handles callouts of signalling failures during the peak passenger travel times, with the result that the MTBF decreases and MTTR might increase accordingly due to the lack of pro-active preventative maintenance.

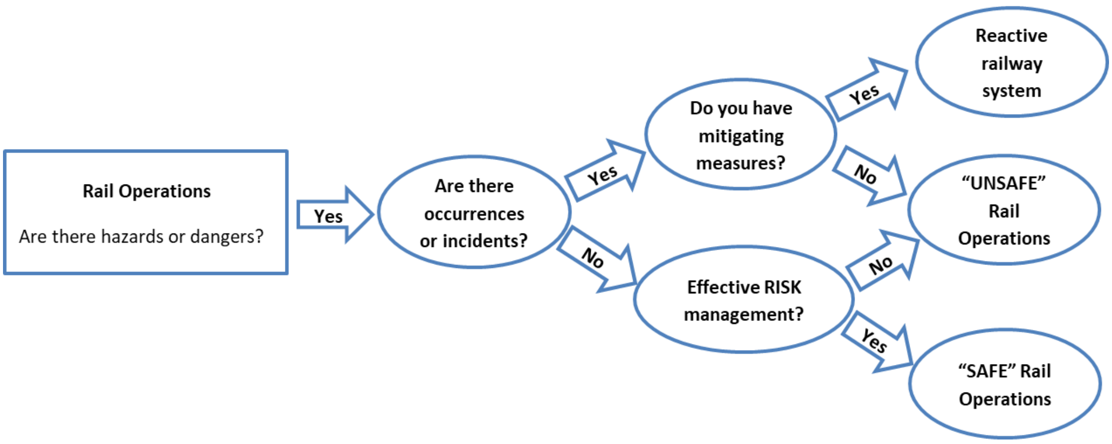



*Figure 1: Decision Tree to determine the Safe Condition of a Railway System (Sprong,2018)*

- If the answer to the question of mitigation measures is negative (see branch B), then the railway system is an “unsafe railway system”.

- If the answer to the question of whether there are occurrences or accidents (or relatively few as was the case on the Sishen-Saldanha line in the past) and the answer is negative or few, then the question is posed whether effective risk management is in place. If the answer is negative (see branch C), then the railway system is an “unsafe railway system”. The reason being that hazards exist, but the collective contributory effect of incidences has just not culminated in resulting in an occurrence or accident, but the probability is high!

- If effective Risk Management practices are in place, (see branch D), then the railway system is considered a “safe railway system”, although hazards do exist.

## 1.2 Railway Safety Risk Model (SRM)

The Railway Safety Risk Model is intended to estimate railway risk for the South African Railway Industry. It is also intended to benchmark the industry safety risk to national safety risk.

The intended objectives of a Safety Risk Model (SRM) are potentially far-reaching, from providing inputs into risk assessments, to assisting in the making of safety decisions about changes or modifications and new infrastructure investment. It is imperative that an examination of the SRM is made, prior to it being extensively used.

The scope of an SRM must be clearly defined with the primary objectives being:

- to provide an understanding of the nature of the current risks in the South African Railway Environment; and
- to provide risk information relating to the various operators that are licenced through the Railway Safety Regulator.

## 1.3 Hazard and Risk

Hazard and risk are used interchangeably in everyday vocabulary. Nevertheless, it has proved useful to the Health & Safety Executive (HSE) to make a conceptual distinction between a hazard and a risk by describing a hazard as the potential for harm arising from an intrinsic property or disposition of something to cause detriment, and risk as the chance that someone or something that is valued will be adversely affected in a stipulated way by the hazard. (HSE – Reducing Risks, Protecting People, 2001)

HSE frequently makes use of the above conceptual distinction in its guidance by requiring that hazards be identified, the risks they give rise to are assessed and appropriate control measures introduced to address the risks. This reflects the fact that in most cases it makes sense to take account of the circumstances in which people and management systems interact with a hazard.

It is often possible to regard any hazard as having more remote causes which themselves represent the ‘true hazard’. For example, when considering the risk of explosion from the storage of a flammable substance, it can be argued that it is not the storage per se which is the hazard, but the intrinsic properties of the substance stored. Nevertheless, it makes sense to consider the storage as the basis for the estimation of risk since this approach will be the most productive one in identifying the practical control measures necessary for managing the risks

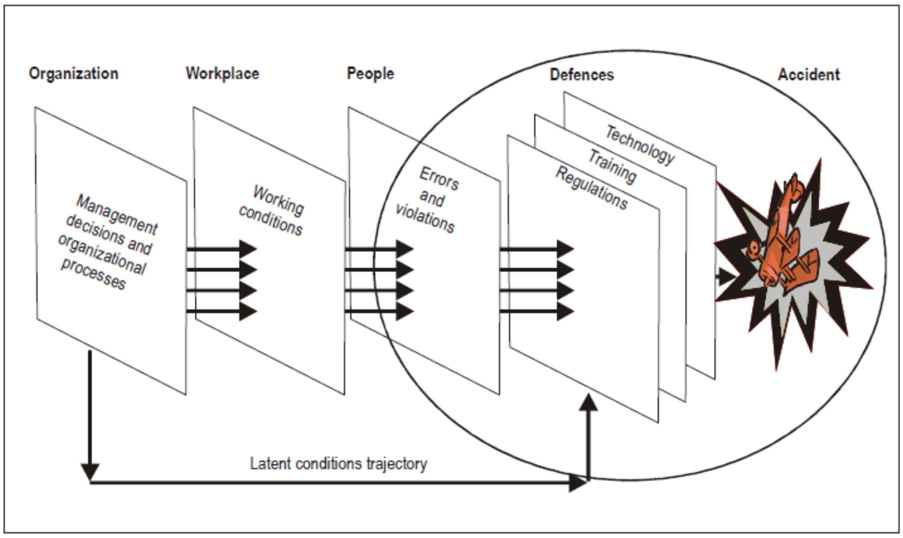
## 1.4 The Chain of events leading to an occurrence or accident.

The hazards in the railway system, are activated into an incident, where an incident is an unplanned, undesired event that hinders the completion or safe execution of a train movement mission and may cause injury, illness, or property damage or some combination of all three in varying degrees from a minor occurrence to a catastrophic occurrence or accident. This is illustrated in Figure 2: Chain of events and RISK elements.


*Figure 2: Chain of events and RISK elements*

## 1.5 Cause of Accidents

The Swiss-Cheese Model, developed by Professor James Reason, illustrates that accidents involve successive breaches of multiple system defences. These breaches can be triggered by several enabling factors such as equipment failures or operational errors. Breaches in safety defences can be a delayed consequence of decisions made at the highest levels of the system, which may remain dormant until their effects or damaging potential are activated by specific operational circumstances. Under such specific circumstances, human failures or active failures at the operational level act to breach the system's inherent safety defences. The Reason Model proposes that all accidents include a combination of both active and latent conditions.




*The concept of accident causation (Safety Management Manual, International Civil Aviation Organisation (2006))*

Risk is a combination of the impact that the incident will have and the probability that it will occur as shown in this equation.

RISK (R) = IMPACT (I) X PROBABILITY (P)

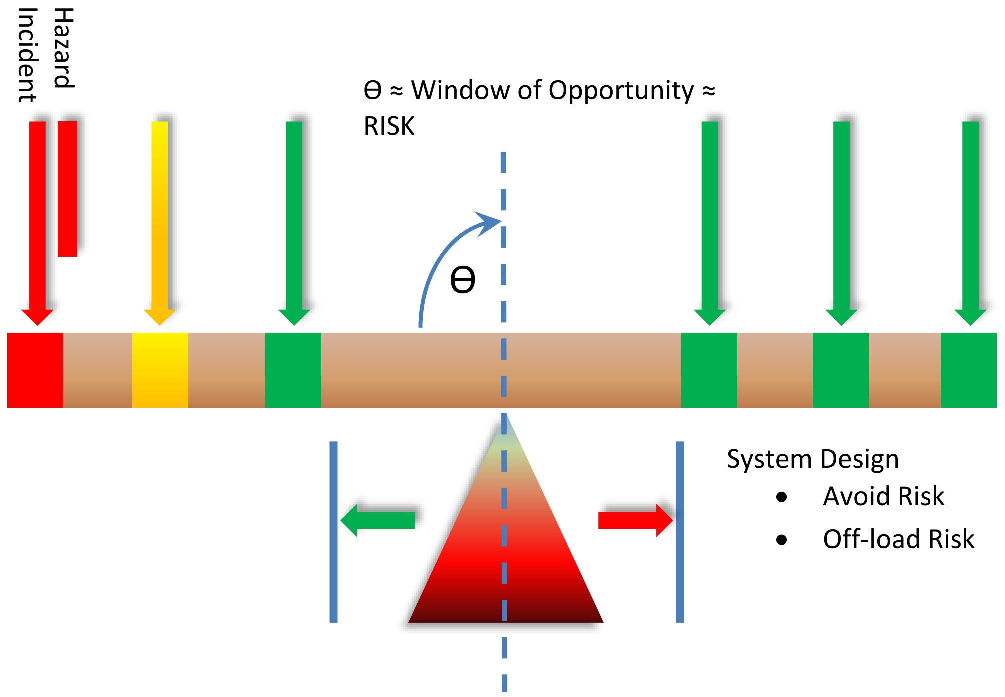



*Figure 3: Risk balance beam model*

Accidents are incidents which occur and result in harm to a person or damage to equipment or property. For an accident, or occurrence, a sum of incidents must occur. This is explained in

***Figure** 3: Risk balance beam model*.

A hazard exists as a potential incident, but until it is transferred to the balance beam by the actions of a human, it has no effect on the potential risk. Once human intervention, or error, causes the hazard to turn into an incident in starts to affect the balance. This balance (ϴ) indicates the probability of an accident occurring. Each hazard that turns into an incident will have an impact (I) and a probability (P). This is explained in Figure 4. This figure is a classification of the risk of an incident, or accident, depending on the level of assessment that is being done.

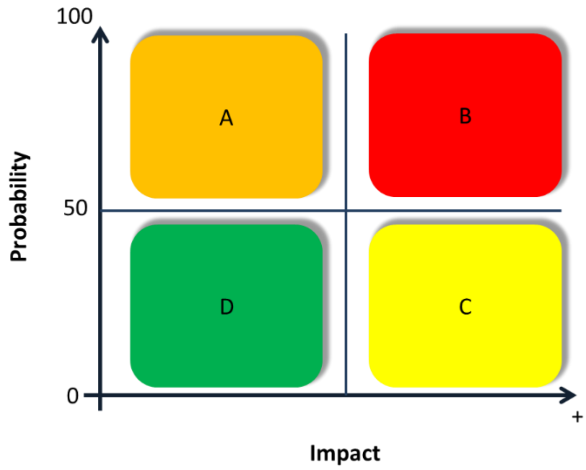



*Figure 4: Relationship between impact and probability*

The triangle at the bottom of the beam (

*Figure **3***) is the influence of human resourcing. This influence will shift the balance. It can cause incidents to have a different effect on risk. The angle, ϴ, is an indication of risk. The wider ϴ becomes, the higher the risk of an accident to occur.

All mitigating efforts are placed on the opposite side of the beam. Figure 1 shows that mitigating efforts will have a variable impact on the balance. This can also be described as the efficiency and effectiveness of the mitigating input. The balance of the system can be influenced during design already.

# 2 *Hazardous Events*

A Hazardous Event (HE) is an incident that has the potential to be the direct cause of safety harm. Railway occurrences must be recorded and reported to the relevant Railway Safety Regulator in the categories numbered from A to O, according to SANS 3000-1 (2016) and the proposed amendment to the Occurrence Reporting Regulation. These railway occurrences must reflect the number of occurrences and not the consequences thereof. Section 5.4 (Reporting of Railway events, including immediate and contributory cause) of SANS 3000 provides a good guideline for identifying precursor to hazardous events.

For the development of a hazard log for the South African railway industry, it is suggested to use two types of hazardous events.

The core hazard categories for **Hazardous Events Operational (HEO)** are:

- Category A: Collisions during movement of rolling stock
- Category B: Derailments during movement of rolling stock

- Category C: Unauthorized movements (rolling stock movements exceeding the limit of authority in respect of position or speed (or both))
- Category D: Level crossing occurrences
- Category E: Persons struck during movement of rolling stock (other than at level crossings)
- Category F: People related occurrences: trains outside station platform areas (in section)
- Category G: Passenger-related occurrences: passengers travelling outside designated passenger area of train
- Category H: People-related occurrences: station platform-train Interchange
- Category I: People — Related occurrences: station infrastructure
- Category J: Electric shock occurrences
- Category K: Spillage or leakage, explosion or loss of dangerous goods
- Category L: Fires
- Category M: Procedural Irregularities (Near Misses)
- Category N: Pantograph Hook-up's
- Category O: On-Board Passenger Related Occurrences

The core hazard categories for **Hazardous Events Safety (HES)** are:

- Category 1: Theft of assets;
- Category 2: Malicious damage (vandalism) to property;
- Category 3: Threats;
- Category 4: Unauthorised Control of trains;
- Category 5: Crowd-related incidents;
- Category 6: Industrial action;
- Category 7: Personal safety on trains;
- Category 8: Personal safety on stations;
- Category 9: Personal safety outside station platform areas; and
- Category 10: Body of dead person dumped within the railway reserve.

Operators and Railway Safety Regulator staff have been using these categories to capture occurrence data and it makes logical sense to build on this experience and understanding when developing the hazard log. The National Information Management System (NIMS) is setup to receive data accordingly.

# 3 Development of a railway Hazard Log

Creating a Hazard Log is a process beginning with some preliminary steps to ensure the existence of an adequate infrastructure for its development. A Hazard Log can be generated from different tools. The first step to be performed is to determine the appropriate method to generate the Hazard Log. Secondly, it is important to appoint an administrator who will be responsible for maintaining, updating and setting up the Hazard Log. Finally, the Hazard Log is established, including activities such as risk classification, state definitions and other general activities to ensure that the operation of the Hazard Log is appropriate.

Once the initial steps are completed, the information entry process will begin, starting with the following steps. The first step to be carried out is hazard identification, which can be obtained from a Preliminary Hazard Analysis (PHA). An accident sequence associated with the hazards identified in the previous step must be developed and a risk assessment must be carried out for each sequence of accidents. The next step is identifying the mitigation factors and register the appropriate ones that has been agreed upon for each accident. Roles and responsibilities must be indicated to the persons overseeing the control of the mitigation factors.

A validation will be performed to detect other hazards or accident sequences related to the hazard in question. This will ensure a complete view of the chain of events that lead to each identified accident.

The process of developing a hazard log is shown in Figure 5. The indicators that are data from the reports by operators to the Railway Safety Regulator in the form of occurrence data is analysed through the preliminary hazard analysis. This is also known as the Failure Mode, Effect and Criticality Analysis (FMECA) and is the start of the Fault Tree Analysis (FTA) process. The accident sequence, or chain of events, is created and reported as an incident log. A HAZOP process identify the leading indicators that is registered in the hazard log.

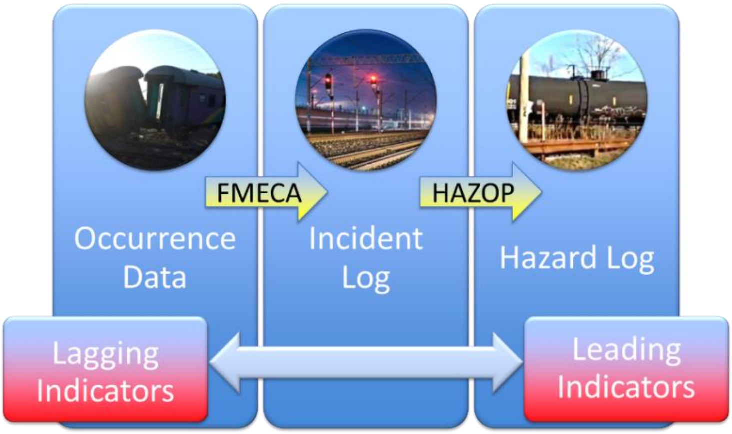



*Figure 5: Hazard log process*

## 3.1 The FMECA Process

The Failure Mode, Effect and Criticality Analysis (FMECA) is an essential first step in understanding the system through the evaluation of the design, operation and environment of the system. The cause-and-effect relationship leading to the core event must be identified and understood. Figure **6** illustrates the importance of the FMECA process in developing a hazard log. The physical boundaries of the system, as defined in the system definition will determine which parts of the system are included in the analysis, and which parts are not. It will include what types of external stresses on the system needs to be analysed, for example war, sabotage, earthquake, lightning, etc.

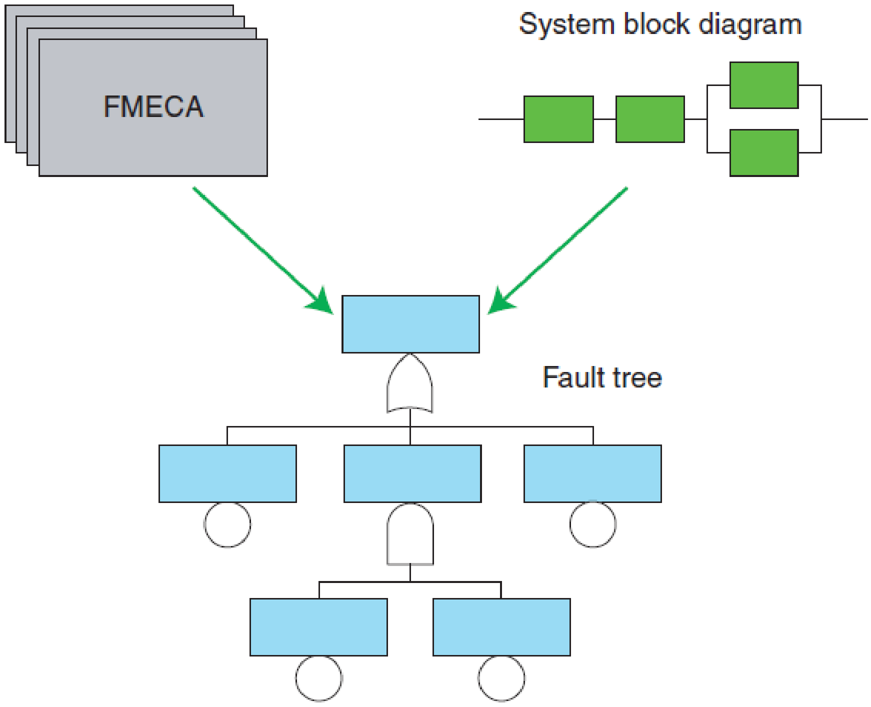



Figure 6: Hazard identification process (Rausand, 2019)

According to ASEMS (2020), a hazard Log contains the traceable record of the Hazard Management process and therefore:

- Ensures that the System Safety Programme uses a consistent set of Safety information;
- Facilitates oversight by the Railway Safety Regulator and other industry stakeholders of the current status of the Safety activities;
- Supports the effective management of possible Hazards and Accidents so that the associated risks are brought to and maintained at a tolerable level; and
- Provides traceability of Safety decisions made.

The FMECA is performed to identify possible problems that could develop because of system failures. The FMECA is oriented to equipment and does not cover the effects of human actions on equipment. The objective is to determine the ways in which equipment can fail, and the effects of such failures on other elements of the system, (Benjamin S. Blanchard, Systems Engineering and Analysis, 1981). Failure effects can be considered at more than one level, for example, at subsystems or the entire system.

FMECA can be based on a hardware or a functional approach. In the hardware approach actual hardware failure modes are considered, for example a resistor that goes open circuit or a bearing seizure. The functional approach is used when hardware items cannot be uniquely identified, (O'Connor, Practical reliability engineering). A combination of the two approaches can also be used.

To perform an effective FMECA, a thorough knowledge of the system is needed. The first step therefore is to obtain all information available on the system. The system definition is described in the consolidated reports for December 2021 and January 2021 for the project to develop the hazard log in context with the hazard identification process for the development of a hazard log.

An FMECA can be performed from different viewpoints, such as safety, mission, success, availability, repair cost, failure mode, etc. The FMECA must include the following information:

- Item identification – Identify each significant system component that is likely to fail.
- Description of failure modes – Define the most probable modes of failure for each identified item. Failure modes are related to the operational modes that the system experiences through the performance of its designed function.
- Cause of failure – The anticipated cause of failure should be described for each instance.
- Possible effects of failure – Describe the most probable effects because of each failure. Effects may range from complete system destruction to partial system operation.
- Probability of occurrence – Through statistical means, estimate the probability of failure occurrence. Probabilities of occurrence may initially evolve from experience factors or through reliability allocation and will be based on reliability prediction data as more date is captured as the system progresses.

Criticality of failure – Failures may be classified in terms of severity in any one of four categories (SANS 3000), depending on the defined failure effects based on

- Table 1.
- Possible corrective action or preventive measures – Describe the action than can be initiated to reduce the probability of failure occurrence or to minimize the effect of failure.

### Table 1: Severity categories (SANS 3000)

| Severity rating scale | | |
|---|---|---|
| Severity | | Rating |
| Negligible | Minor Injury, slight repairable damage to assets, limited damge to minimal area of low significance to the environement. | 1 |
| Marginal | Minor Injury requiring hospitalisation, minor damage to assets that is mostly repairable, minor effect on biological or physical environement | 2 |
| Moderate | Moderate injury or occupational illness, moderate damage to assets, moderate (short-term) effects to environment but not effecting ecosystem function | 3 |
| Critical | Single fatality or severe irreversable disability to one of more person, major damge to the assets, serious medium term environmental effects. | 4 |
| Catastrophic | Multiple fatalities or significant ireeversable effects to persons, extensive damage to assets, very serious, long-term environemental imparment of ecofuntion | 5 |

## 3.2 The HAZOP process

A Hazard and Operability (Hazop) study is an important technique used in risk and reliability assessments of railway systems. Due to the complexity of a railway system, it is important that design and operational hazards are not missed. Furthermore, identifying hazards during the design phase will ensure that safety and operability risks are reduced.

A Hazop is a structured and systematic technique for identifying hazards and operability problems throughout the system. It is particularly useful in identifying unforeseen hazards designed into systems due to lack of information or introduced into existing systems due to changes in process conditions or operating procedures.

Use of the Hazop Analysis technique requires a detailed source of information concerning the design and operation of system. A Hazop is a qualitative technique based on guidewords or deviations and is carried out by a multi-disciplinary team (industry working group) during a set of meetings.

During the Hazop study a high-level Fault Tree Analysis (FTA) will be performed, whereby a graphical representation of possible causes of core events will be developed.

The purpose of a HAZOP study is to identify and assess the potential hazards to safety in the

Railway system as well as identify potential operating problems. It is an opportunity to identify precursor events that will trigger action that will prevent undesirable occurrences. In particular, the HAZOP study is to:

- Determine how the system might deviate from the design intent (See the definition for Reliability);
- Identify all potential causes of process upset scenarios which could lead to significant safety or operability consequences (FTA);
- Ensure that the risk from each identified scenario is at as low as reasonable acceptable level (ALARP);
- Recommend modifications or adjustments that will reduce the risk to a reasonable acceptable low level, or specify a further study to investigate the issue, with the objective of identifying a suitable modification or adjustment.

It is important to note that a Hazop study is an identifying technique and not intended as a means of solving problems. Section 1.2 describes a proposed Safety Risk Model (SRM) for the railways in South Africa. It is important to note that risk is a combination of the likelihood that and event will occur and the impact (severity) that it will have on the reliability of the system.

The following essential steps shall be followed in performing the HAZOP study for this project:

- Select a study node or path based on the SANS 3000 categories. These are described in the hazard log as the sub hazard events and are included in Table 2;
- Apply guide-words/deviations to determine the precursors to the hazard event;
- Evaluate causes, consequences/problems and safeguards in place and risk as described in Section 3.
- Recommend controls to be actioned that includes: What? When? Who?
- Record information in the Hazard log

**Table 2: Sub hazard event description (SANS 3000)**

| | |
|---|---|
| A-a | Collision between rolling stock on a running line |
| A-b | Collision of rolling stock with an obstruction on a running line (including road vehicles colliding with rolling stock) |
| A-c | Collision with a stop block on a running line |
| A-d | Collision of rolling stock other than on a running line |
| A-e | Collision of rolling stock with an obstruction other than on a running line |
| A-f | Collision with a stop block (other than on a running line) |
| B-a | Derailment of rolling stock on a running line |
| B-b | Derailment of rolling stock on a line other than a running line |
| B-c | Derailment during tippler activities |
| C-a | Signal passed at danger (SPAD) on a running line |
| C-b | Signal passed at danger (SPAD) on any other line |
| C-c | Physical token passed on a running line |
| C-d | Physical token passed on any other line |
| C-e | Verbal authority exceeded on a running line |
| C-f | Verbal authority exceeded on any other line |

| | |
|---|---|
| C-g | Written authority exceeded on a running line |
| C-h | Written authority exceeded on any other line |
| D-a | Collision between rolling stock and a road vehicle(s) (including motor vehicles, bicycle or animal-drawn vehicles) at a recognized level crossing on a running line |
| D-b | Collision between rolling stock and a road vehicle(s) (including motor-powered, bicycle or animal-drawn vehicles) on any line other than a running line (including yards, sidings and private sidings) at a recognized level crossing |
| D-c | A person(s) struck by rolling stock at a recognized pedestrian level crossing |
| D-d | A person(s) struck by rolling stock at a recognized road level crossing |
| E-a | Occurrence where a member of the public is struck by rolling stock on a running line |
| E-b | Occurrence where an employee is struck by rolling stock on a running line |
| E-c | Occurrence where a contractor or contractor's employee is struck by rolling stock on a running line |
| E-d | Occurrence where a member of the public struck by rolling stock on a line other than a running line |
| E-e | Occurrence where an employee is struck by rolling stock on a line other than a running line |
| E-f | Occurrence where a contractor or contractor's employee is struck by rolling stock on a line other than a running line |
| F-a | Occurrence where a person fell or was pushed from inside a moving or stationary train |
| F-b | Occurrence where an employee fell or was pushed from inside a moving or stationary train |
| F-c | Occurrence where a contractor or contractor's employee fell or was pushed from inside a moving or stationary train |
| G-a | Category G occurrences covers the number of occurrences as a result of passengers travelling outside the designated passenger area of the train |
| H-a | Occurrence where a passenger fell between the train and the platform whilst entraining/detraining a stationary or moving train |
| H-b | Occurrence where a passenger fell on the platform whilst entraining/detraining a stationary or moving train |
| H-c | Occurrence where an employee fell between the train and the platform whilst entraining/detraining a stationary or moving train |
| H-d | Occurrence where an employee fell on the platform whilst entraining/detraining a stationary or moving train |
| H-e | Occurrence where a contractor or contractor's employee fell between the train and the platform whilst detraining a stationary or moving train |
| H-f | Occurrence where a contractor or contractor's employee fell on the platform whilst entraining/detraining a stationary or moving train |
| I-a | Occurrence resulting in injuries and fatalities to public due to infrastructure defects in a public area of the station |
| I-b | Occurrence resulting in injuries and fatalities to passengers due to infrastructure defects in a passenger area of the station |
| I-c | Occurrence resulting in injuries and fatalities to an employee due to infrastructure defects in a public area of the station |
| I-d | Occurrence resulting in injuries and fatalities to an employee due to infrastructure defects in a passenger area of the station |
| I-e | Occurrence resulting in injuries and fatalities to a contractor or contractor's employee due to infrastructure defects in a public area of the station |
| I-f | Occurrence resulting in injuries and fatalities to a contractor or contractor's employee due to infrastructure defects in a passenger area of the station |
| J-a | Electrical shock to a member of the public on the network infrastructure |

| | |
|---|---|
| J-b | Electrical shock to an employee on the network infrastructure |
| J-c | Electrical shock to a contractor or contractor's employee on the network infrastructure |
| J-d | Electrical shock to the member of the public including passengers whilst on or in rolling stock |
| J-e | Electrical shock to an employee whilst positioned on or part of rolling stock |
| J-f | Electrical shock to a contractor or contractor's employee whilst positioned on or part of rolling stock |
| J-g | Electrical shock to the member of the public in the public area of a station |
| J-h | Electrical shock to an employee in the public area of a station |
| J-i | Electrical shock of a contractor or contractor's employee in the public area of a station |
| J-j | Electrical shock to the member of the public in the passenger area of a station |
| J-k | Electrical shock to an employee in the passenger area of a station |
| J-l | Electrical shock of a contractor or contractor's employee in the passenger area of a station |
| K-a | Spillage or leakage of dangerous goods en route |
| K-b | Spillage or leakage of dangerous goods during shunting operations |
| K-c | Spillage or leakage of dangerous goods whilst staged |
| K-d | Missing consignment of dangerous goods |
| K-e | Theft of dangerous goods |
| K-f | Explosion of dangerous goods |
| L-a | Fires on a fixed operational asset ( for example, station buildings, in a tunnel, in a relay room and in a sub-station) |
| L-b | Fire of freight |
| L-c | Fire of rolling stock |
| L-d | Veld fires that threaten operational safety |

The Hazard process is shown in Figure 7. This is the prescribed process that is used by ESKOM (PGZ 45-24 Hazop Guideline). It clearly indicates the similarity to an FTA process.

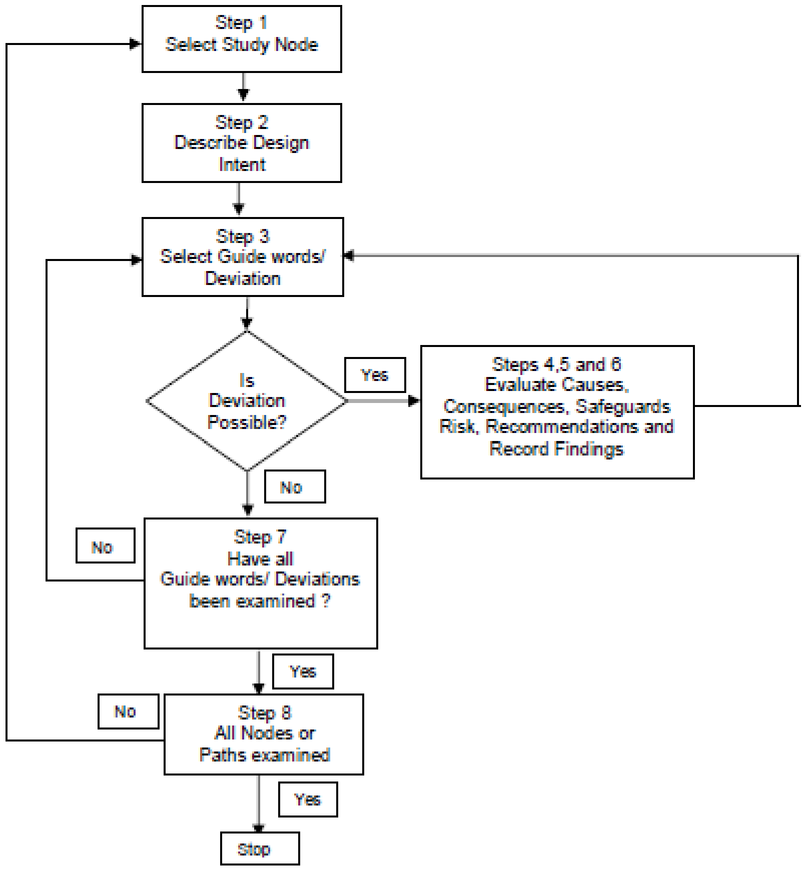



**Figure 7: Hazop Study process (Eskom, PGZ 45-24)**

Analysing the frequency of the hazards begins with the basic events frequency and proceeds toward the top event in FTA. The basic event frequency or probabilities is gathered from the expert judgments in the industry working groups.

Table 3 shows the categories for the frequency and compares it to a probability (likelihood) rating based on SANS 3000-1. The industry working group will confirm the proposed rating based on their expert judgement.

FTA is a deductive approach that consists of symbols and gates to describe the process of system failure. To analyse the fault tree, the evaluations use the rules of Boolean Algebra. The Hazop process and FTA is carried out to find the root cause of potential failure until the controllable cause is reachable.

During the development of the hazard log, the Hazop process will be completed to quantify risk before controls are implemented. The risk rating will be determined by multiplying likelihood and severity based in

Table 1 and

Table 3. This will be used as a weighted risk for each category to enable the use of the precursor hazard events to trigger actions in the prevention of unwanted occurrences.

### Table 3: Frequency rating for hazardous events (SANS300)

| Likelihood rating scale | | | |
|---|---|---|---|
| Hazard Likelihood description | | Hazard Frequency | Rating |
| Improbable | Hazardous event is so unlikely to occur, it can be assured occurrence will not be experienced but is possible in a group of items | Not in 100 years | 1 |
| Remote | Hazardous event unlikely, but possible to occur in the lifetime of an item or might be expected to occur in a group of items | Once in between 10 years and 100 years | 2 |
| Occasional | Hazardous event likely to occur sometime in the life of the equipment or will occur several times in a group of items | Once in between 1 year and 10 years | 3 |
| Probable | Hazardous event will occur several times in the life of an item or will occur frequently in a group of items | Once in between 1 month and 1 year | 4 |
| Frequent | Hazardous event is likely to occur frequently in the life of an item or is continuously experienced in a group of items | Once or more per month | 5 |

The risk rating for each hazard is calculated by multiplying the likelihood and severity rating as shown in **Error! Not a valid bookmark self-reference.**. Where a rating between 1 and 3 will be classified as a LOW risk, between 4 and 10 a MEDIUM risk and above 10 a HIGH risk.

### Table 4: Risk rating

| | Negligible | Marginal | Moderate | Critical | Catastrophic |
|---|---|---|---|---|---|
| Improbable | 1 | 2 | 3 | 4 | 5 |
| Remote | 2 | 4 | 6 | 8 | 10 |
| Occasional | 3 | 6 | 9 | 12 | 15 |
| Probable | 4 | 8 | 12 | 16 | 20 |
| Frequent | 5 | 10 | 15 | 20 | 25 |

# 4 Information technology requirement

The process for developing a Hazard Log requires several initial steps to be undertaken prior to Hazard Log population. This is to ensure that there is a suitable infrastructure in place before Hazard information is stored.

- A method by which the Hazard Log is to be implemented must be selected. This can either be in paper or electronic form. It is important at the outset to identify the appropriate tool/administration method for the Hazard Log.
- A Hazard Log administrator must be appointed. The Hazard Log administrator will be responsible for the maintenance, upkeep and configuration control of the Hazard Log. All non-administrators should be allowed read only access if the Hazard Log is in electronic format.

A system requirement is based on the draft hazard log example in Annexure **Error! Reference source not found.** and the process described to develop and maintain the log in future. The diagram in Figure 8 summarises the requirements for the information technology requirements.

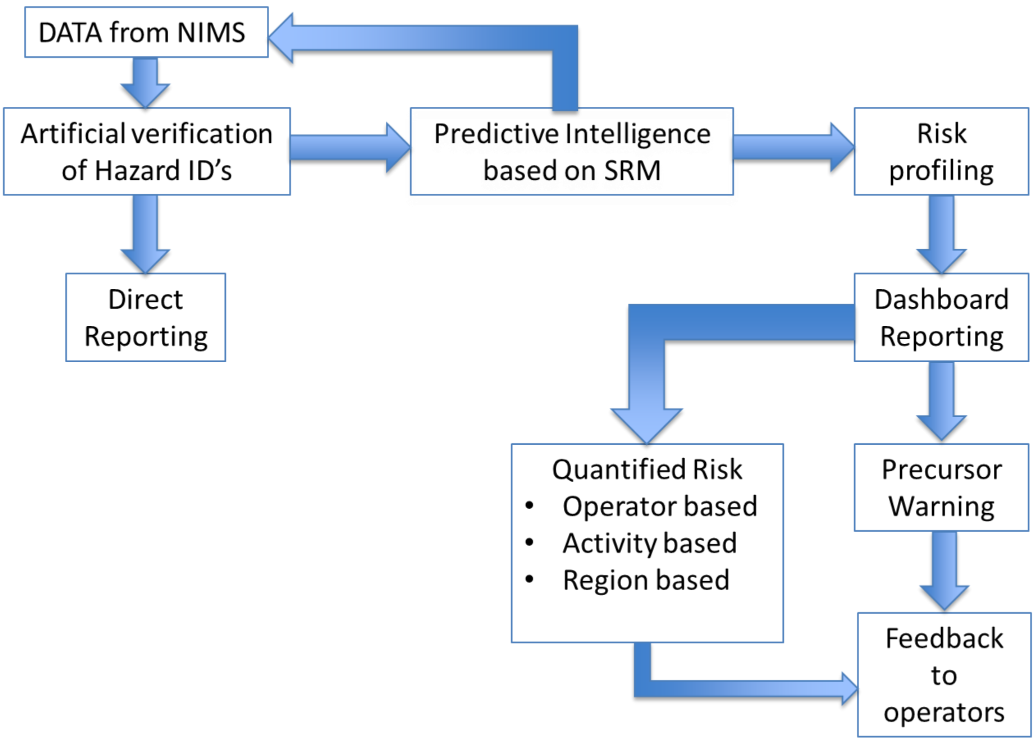



Figure 8: System requirement

### 4.1.1 Data from the National Information Management System (NIMS)

Precursor to hazardous event data must be logged in NIMS based on hazard log identification codes as shown in the example in **Error! Reference source not found.**. It is required that the interface with user must have a separate level of authentication to allow for more operator staff to be able to log precursors or "near misses" to hazardous events.

A near miss is an incident which results to no injury, no damage to property/equipment/machinery, and no environmental effect but has the potential for all those. It is a potential occurrence. It is mostly overlooked on site because it presents no negative impact. Though it poses no immediate negative impact, it can present a trend of events which may result to serious damage and losses if properly investigated.

Occurrence and Hazard data will be compared to proof and improve trends analysis to trigger actions required for the prevention of railway incidents and occurrences.

#### 4.1.2 Artificial verification of Hazard ID's

Data from NIMS must be verified against a set of rules based on the Hazard log. For example, to ensure that precursor hazard ID's correspond with the core and sub hazard events.

User ID's will be verified, and data analysed to find possible trend in the incorrect logging by certain users. Although logging will not be anonymous, the information will be protected to ensure that staff are comfortable to report incidents.

The verified data will be imported into the SRM to enable the quantification of risk through the model. Direct, or manual, reporting must be possible by exporting data to Microsoft Excel. This is required for the quarterly quality audits during which the integrity of the system will be proofed.

#### 4.1.3 Predictive intelligence based on the Safety Risk Model (SRM)

- Hazard ID's must be grouped and allocated against the occurrence categories where each will have a negative impact once activated;
- Weighted risk based on the risk rating in the hazard log must be calculated;
- Trend analysis to improve the risk rating allocated during the development of the hazard log must be done;
- Feedback into the NIMS system data to enable more accurate calculation based on occurrence data;
- Determine human factor input that activated the risk into an incident; and
- Update severity rating for hazard activated into incidents.

#### 4.1.4 Dashboard ad reporting

- Activation of action to be taken based on risk profile through a precursor warning system;
- Risk profile dashboard to provide visual feedback on the continuous monitoring of the risk through the reporting of the hazards or "near misses"; and
- Feedback to the operators to enable early activation of interventions to prevent occurrences. Operators need to provide feedback on actions taken. Artificial monitoring of actions taken against reporting of hazards to monitor success.