**System Safety Plan**

***Document No.***

***Version. 1.0***

Approval History

|  |  |  |  |
| --- | --- | --- | --- |
|  | Prepared By | Reviewed By | Approved By |
| Name |  |  |  |
| Signature |  |  |  |
| Date |  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version (x.y) | Date of Revision | Description of Change | Reason for Change |
| 0.1 |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Preface 6](#_Toc162890370)

[1.1 Purpose 6](#_Toc162890371)

[1.2 System Overview 6](#_Toc162890372)

[1.3 Definitions 6](#_Toc162890373)

[1.4 Acronyms and Abbreviations 7](#_Toc162890374)

[1.5 References 9](#_Toc162890375)

[2 Safety Policy and Strategy 11](#_Toc162890376)

[2.1 Safety Policy 11](#_Toc162890377)

[2.2 Safety Management Principles 11](#_Toc162890378)

[3 Safety Organization 12](#_Toc162890379)

[3.1 Safety Organization Srtucture 12](#_Toc162890380)

[3.2 Roles and Responsibilities 12](#_Toc162890381)

[3.3 Skill Set 13](#_Toc162890382)

[4 Safety Programme 15](#_Toc162890383)

[4.1 Safety targets 15](#_Toc162890384)

[4.2 Safety Requirements 15](#_Toc162890385)

[4.3 System Life cycle 16](#_Toc162890386)

[4.4 Safety Activities 16](#_Toc162890387)

[4.5 Risk Analysis 20](#_Toc162890388)

[4.6 Hazard Analysis 24](#_Toc162890389)

[4.7 Handling of Systematic faults 31](#_Toc162890390)

[4.8 Safety Review and Audits 35](#_Toc162890391)

[4.9 Safety Analysis of System Maintenance, Performance and Operation 36](#_Toc162890392)

[4.10 Interface with other related programme or plans 36](#_Toc162890393)

[5 Safety case 37](#_Toc162890394)

[5.1 Safety Case Structure 37](#_Toc162890395)

[5.2 Management of SRAC 39](#_Toc162890396)

[5.3 System configuration and System build 39](#_Toc162890397)

[6 Safety Assessment and authorisation Process 43](#_Toc162890398)

[6.1 Safety Assessment Process 43](#_Toc162890399)

[6.2 Safety Authorisation Process 44](#_Toc162890400)

[7 Safety Life Cycle Deliverables 46](#_Toc162890401)

[8 Appendix A: Hazard Analysis Templates 47](#_Toc162890402)

[8.1 Preliminary Hazard Analysis 47](#_Toc162890403)

[8.2 System Hazard Analysis 47](#_Toc162890404)

[8.3 Interface Hazard Analysis 47](#_Toc162890405)

[8.4 Operating & Support Hazard Analysis 48](#_Toc162890406)

[8.5 Hazard Log 48](#_Toc162890407)

**Table of Figures**

[Figure 2: Safety organization structure 12](#_Toc162890334)

[Figure 3: System Life Cycle 16](#_Toc162890335)

[Figure 4: Risk Analysis Process 20](#_Toc162890336)

[Figure 5: ALARP Principle 23](#_Toc162890337)

[Figure 6: PHA Process 26](#_Toc162890338)

[Figure 7: SHA Process 27](#_Toc162890339)

[Figure 8: IHA Process 28](#_Toc162890340)

[Figure 9: FTA Process 29](#_Toc162890341)

[Figure 10: OSHA Process 30](#_Toc162890342)

[Figure 11: Safety Case Structure 37](#_Toc162890343)

**Table of Tables**

[Table 1: Definitions 7](#_Toc162890344)

[Table 2: Acronyms and Abbreviations 9](#_Toc162890345)

[Table 3: References 10](#_Toc162890346)

[Table 4: Safety Manager 13](#_Toc162890347)

[Table 5: Safety Engineer 13](#_Toc162890348)

[Table 6: Skill Set 14](#_Toc162890349)

[Table 7: SIL targets for FNMux System 15](#_Toc162890350)

[Table 8: Frequency of Occurrence of Hazards 21](#_Toc162890351)

[Table 9: Severity of Hazards 21](#_Toc162890352)

[Table 10: Risk Assessment Matrix 21](#_Toc162890353)

[Table 11: Risk Acceptance Categories 22](#_Toc162890354)

[Table 12: Risk Acceptance Criteria 23](#_Toc162890355)

[Table 13: SIL Allocation as per THR 23](#_Toc162890356)

[Table 14: SIL Allocation as per TFFR 24](#_Toc162890357)

[Table 15: Hazard Analysis 25](#_Toc162890358)

[Table 16: Technique/Measure for Design features 33](#_Toc162890359)

[Table 17: Failure and Hazard Analysis Methods 34](#_Toc162890360)

[Table 18: Techniques for Design and development of system, subsystem 34](#_Toc162890361)

[Table 19: Techniques for Safety verification and validation of system and subsystem 35](#_Toc162890362)

[Table 20: Techniques for Safety verification and validation of system and subsystem 35](#_Toc162890363)

[Table 21: Safety Deliverables 46](#_Toc162890364)

[Table 22: Preliminary Hazard Analysis 47](#_Toc162890365)

[Table 23: System Hazard Analysis 47](#_Toc162890366)

[Table 24: Interface Hazard Analysis 48](#_Toc162890367)

[Table 25: Operating & Support Hazard Analysis 48](#_Toc162890368)

[Table 26: Hazard Log 48](#_Toc162890369)

# Preface

## Purpose

The Purpose of this plan is to determine the safety objectives, identify safety organization and processes shall be followed during the overall FNMux System life cycle. This plan identifies suitable safety activities related to system, hardware, and software life cycle of the generic application. It also discusses the demonstration of the generic application system safety via safety case documentation which details the dependent safety cases and ways to manage the safety related application conditions of the dependent generic product.

## System Overview

## Definitions

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 1: Definitions

## Acronyms and Abbreviations

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 2: Acronyms and Abbreviations

## References

The following are the reference documents referred during the preparation of System Requirement Specifications.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table 3: References

# Safety Policy and Strategy

## Safety Policy

To design and develop world-class solutions meeting required safety integrity levels by adopting:

* Effective safety management and inculcating safety culture throughout the organization
* Safety first policy (above functionality, performance & cost) in our decision-making process
* Proactive safety hazards and incident reporting strive to promote our commitment to safety consistently.
* Conformance to relevant safety standards

## Safety Management Principles

* Establish and observe a written corporate safety policy.
* Establish an independent safety review process.
* Establish an independent Safety Management Process group.
* Identify and evaluate the severity and foreseeability of product hazards.
* Conduct a design review assessing the risk of injury by considering the hazards, the environment, and potential use.
* Reduce the risk associated with the hazard to ALARP (As Low as Reasonably Possible).
* Warn the product users, operators, and maintainers, about the Safety Related
* Application Conditions (SRACs) and educate them on accident or hazard prevention.
* Promote, through constant user interaction, training and education, the safe use of a product.
* Maintain safety-related records during the useful shelf life of the product.
* Continuously monitor the safety performance of the product whilst the system is in use.
* Promptly notify product users and institute recall procedures where necessary to substantially reduce or eliminate accidents.
* Conduct safety training and seminars at regular intervals to bring a safety culture to the product design and development organization.
* Monitor and continuously improve the safety management process.

# Safety Organization

## Safety Organization Srtucture

The Safety Organization fulfils the CENELEC standards in compliance with reference to achieve the required safety integrity level. The Safety Organization is structured as follows. Additionally, an external Independent Safety Assessor (ISA) shall certify the system's corresponding safety level.

Figure 2: Safety organization structure

## Roles and Responsibilities

### Safety Manager

| SI | Role | Safety Management |
| --- | --- | --- |
|  | Responsibilities | * Responsible for defining the safety plan and implementation of the plan throughout the project life cycle. * Responsible for the assurance of the system which fulfils the RDSO requirements completely without any anomaly. * Responsible for reviewing the safety plan at appropriate stages in the project life cycle. * Responsible for identifying the necessary safety activities to be conducted for the project life cycle. * Responsible for addressing the safety review meetings and audits conducted by client. * Responsible for the safety verification and validation activities throughout the life cycle. * Responsible for delivering safety verification and validation reports. * Responsible for providing training related to system and safety standards for the personnel who are involved in safety activities. * Responsible to work closely with the Independent Safety Assessor during system acceptance phase. |
|  | Key Competencies | * Shall have competence in Railway Signalling domain and exposure to safety principles. * Shall be thorough in EN 50126, EN 50128, EN 50129 & ISO 9001:2015. |

Table 4: Safety Manager

### Safety Engineer

| SI | Role | Safety activities execution |
| --- | --- | --- |
|  | Responsibilities | * Responsible for conducting the safety activities. * Perform safety hazard analysis during the preliminary and detailed design phases. * Responsible for preparing safety case documents. * Responsible for reporting to Safety manager related to safety activities. * Responsible to update and maintain the hazard log |
|  | Key Competencies | * Shall have competence in Railway Signalling domain and exposure to safety design principles. * Shall be thorough in EN 50126, EN 50128, EN 50129 & ISO 9001:2015. |

Table 5: Safety Engineer

## Skill Set

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI | Name of the Personnel | Role | Skill Set | Responsibility |
|  | XXX | Safety Manager |  | • Responsible for defining the safety plan and implementation of the plan throughout the project life cycle.  • Responsible for the assurance of the system which fulfils the RDSO requirements completely without any anomaly.  • Responsible to review the safety plan at appropriate stages in the project life cycle.  • Responsible to identify the necessary safety activities to be conducted for the project life cycle.  • Responsible for addressing the safety review meetings and audits conducted by client.  • Responsible for the safety verification and validation activities throughout the life cycle.  • Responsible for delivering safety verification and validation reports.  • Responsible to provide training related to system and safety standards for the personnel who are involved in safety activities  • Responsible to work closely with the Independent Safety Assessor during system acceptance phase |
|  | XXXX | Safety Engineer |  | • Responsible for conducting the safety activities.  • Perform safety hazard analysis during the preliminary and detailed design phases.  • Responsible for preparing safety case documents.  • Responsible for reporting to Safety manager related to safety activities.  • Responsible to update and maintain the hazard log. |

Table 6: Skill Set

# Safety Programme

## Safety targets

The FNMux System shall conform to Safety Integrity Level SIL-4 as per CENELEC or equivalent standards as per RDSO specification RDSO/SPN.

The SIL target for FNMux system / sub-systems shall be fixed as per the requirements from the RDSO as per the following table.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SI | Description | Safety Integrity Level | THR | TFFR | RDSO specification |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL -2 | 10-7 < THR < 10-7 | 10-7 < THR < 10-7 |  |
|  |  | SIL - 4 | 10-9 < THR < 10-8 | 10-9 < THR < 10-8 |  |
|  |  | SIL -2 | 10-7 < THR < 10-7 | 10-7 < THR < 10-7 |  |

Table 7: SIL targets for FNMux System

The Safety critical functions shall be identified through safety analyses and SIL target for each function shall be allocated and documented separately.

## Safety Requirements

The safety requirements for the system shall be established in the following ways.

* The requirements provided by the RDSO in the specification.
* The requirements shall be extracted from the mitigation action prescribed in the hazard analysis process.
* The requirements from the safety study of a similar system or experience from the same system.
* All the critical safety function SIL shall be established by the causal analysis method.
* The safety requirements associated with system interface shall be identified through Interface hazard analysis.
* The responsibility of the safety function associated with system interface shall be identified. If the interface safety function needs to be managed by another contractor, the requirement shall be intimated formally to the other contractor and finalize the responsibility for the management of the safety function with mutual study and understanding.

## System Life cycle

A diagram of a system

Description automatically generated

Figure 3: System Life Cycle

## Safety Activities

This section presents the summary of the FNMUX product’s phases and documents to be prepared throughout the development of the entire product at system level to provide the demonstration of the safety level at each phase of the product.

The product phases are defined as follows:

1. Concept

2. System definition and operational context

3. Risk analysis and evaluation

4. Specification of System Requirements

5. Architecture and apportionment of System requirements

6. Design and implementation

7. Manufacture

8. Integration

9. System validation

10. System acceptance

11. Operation and maintenance

As part of the safety program, the safety team shall carry out Kavach product’s safety activities. The following table discusses the safety activities to be conducted for the system life cycle.

| SI | Lifecycle phase | Phases related Safety tasks | System Safety deliverables | Responsibility |
| --- | --- | --- | --- | --- |
|  | Concept | Review previously achieved safety performance.  Consider the safety implications of the project.  Review the Safety Policy and Safety Targets. | No deliverable | Safety Manager |
|  | System Definition and Application Conditions | Evaluate experience data for safety.  Perform the Preliminary Hazard Analysis.  Establish the Safety Plan (overall).  Define the risk acceptance criteria.  Identify the influence on the system safety of the existing infrastructure constraints. | Preliminary hazard Analysis  System Safety Plan | Safety Manager,  Safety Engineer |
|  | Risk Analysis | Perform Risk analysis.  Perform Risk evaluation.  Set up the hazard log. | Hazard Log | Safety Manager,  Safety Engineer |
|  | System Requirements | Specify the System Safety Requirements with their corresponding SIL.  Define the safety acceptance criteria (overall).  Define the safety-related functional requirements of the system.  Establish the safety management.  Manage the Safety verification and validation through V&V plan. | System Safety plan  System Safety Requirements Specification  Quality Management Report (Safety Case)  Phase level verification report | Safety Engineer |
|  | Apportionment of System Requirements | Apportion System Safety Targets and Requirements.  Specify the Sub-systems and Components safety requirements.  Determine SIL for Subsystems and its components.  Define the Sub-systems and Components acceptance criteria. |
|  | Design and Implementation | Implement the FNMux Safety Plan by review, analysis, testing and data assessment, addressing:  Hazard Analysis  Hazard Log  (System hazard Analysis (SHA),  Interface Hazard Analysis (IHA),  Operation & Support Hazard Analysis (OSHA),  Fault Tree analysis (FTA))  Justify the safety-related design decisions.  Undertake the Safety Program  Control, covering.  Prepare (if appropriate) the Generic Application Safety Case. | Safety Review  System Hazard Management and Logging  Hazard Analyses  (SHA  IHA  OSHA  FTA)  Hazard Log  Safety Management Report (Safety Case)  Phase level verification report | Safety Manager,  Safety Engineer |
|  | Manufacturing | Implement the Safety Plan by review, analysis, and testing and data assessment.  Use the Hazard Log.  System functional and safety verification | Technical Safety Report (Safety Case)  Phase level verification report | Safety Engineer,  Safety Manager |
|  | Installation | Establish the Installation Safety Program.  Implement the Installation safety Program.  Installation verification activity |
|  | System Validation (Including Safety Acceptance and Commissioning) | Perform functional testing of the system.  Perform Pre-Commissioning checks.  Establish the Commissioning Program.  Implement the Commissioning Program.  Validation of the system against client requirements | System Test Report.  System Validation Report  System Safety Case | RAMS V & V,  Safety Engineer  Safety Manager |
|  | System Acceptance | Assess Generic application Safety Case | ISA report | BV |
|  | Operation & Maintenance (Including Performance Monitoring) | Undertake on-going safety centered maintenance.  Perform on-going safety performances monitoring and Hazard Log maintenance.  Collect, analyze, evaluate, and use performance and safety statistics. | System Assurance Report | Safety Engineer |

## Risk Analysis

As mentioned in the above table, FNMux risk analysis is a process of risk assessment and acceptance process. The risk assessment process identifies the risk level of the identified hazard. The risk acceptance process guides the principle to accept the risk associated with the system.



Figure 4: Risk Analysis Process

The Risk is a combination of Frequency of occurrence of hazards and severity of hazards. The following frequency of occurrence of hazard and severity of hazards shall be used for the estimation of risk level associated with each hazard.

### Frequency of Occurrence of Hazards

The classification of the frequency of is as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Frequency | Description | Frequency Range |
| A | Frequent | Likely to occur frequently. The event will be frequently experienced | Once in 6 weeks |
| B | Probable | Will occur several times. The event can be expected to occur often | Once per 6 weeks to a year |
| C | Occasional | Likely to occur several times. The event can be expected to occur several times | Once per 1 year to 10 years |
| D | Rare | Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur | Once per 10 years to 1000 years |
| E | Improbable | Unlikely to occur but possible. It can be assumed that the event may exceptionally occur | Once per 1000 years to 100000 years |
| F | Highly  improbable | Extremely unlikely to occur. It can be assumed that the event will not occur | Once in 100000 years or more |

Table 8: Frequency of Occurrence of Hazards

### Severity of Hazards

The following severity levels shall be used to classify the severity of the consequences of the hazards.

|  |  |  |
| --- | --- | --- |
| Category | Frequency | Frequency Range |
| I | Catastrophic | Multiple fatalities, Extreme damage to environment, Major system loss, Severe system damage, Minor system damage |
| II | Critical | At least one fatality, large damage to environment, Loss of major system |
| III | Marginal | No Fatality, Minor damage to environment, Severe system damage |
| IV | Insignificant | Minor injury, Minor system damage |

Table 9: Severity of Hazards

### Risk Assessment

The aim of the risk assessment is to identify the risk level of the hazards associated with the FNMux system. Hazards in the FNMux system shall be identified based on a set of safety analysis conducted all along the lifecycle.

The following risk assessments matrixes shall be considered while estimating the risk category. It also shows the various zones of acceptability of the risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity  **Occurrence** | Catastrophic  (I) | Critical  (II) | Marginal  (III) | Negligible  (IV) |
| Frequent (A) | Intolerable | Intolerable | Intolerable | Undesirable |
| Probable (B) | Intolerable | Intolerable | Undesirable | Tolerable |
| Occasional (C) | Intolerable | Undesirable | Undesirable | Tolerable |
| Rare (D) | Undesirable | Undesirable | Tolerable | Negligible |
| Improbable (E) | Undesirable | Tolerable | Negligible | Negligible |
| Highly Improbable (F) | Tolerable | Negligible | Negligible | Negligible |

Table 10: Risk Assessment Matrix

### Risk Acceptance Principle

The following table shows the risk acceptance indices. The risks of Intolerable category shall be eliminated with proper mitigation action. For other risk levels appropriate actions shall be considered as per the table below.

|  |  |
| --- | --- |
| Risk Acceptance Category | Actions to be applied |
| Intolerable | The risk shall be eliminated |
| Undesirable | The risk shall only be accepted if its risk reduction is impracticable |
| Tolerable | The risk can be tolerated and accepted with adequate control |
| Negligible | The risk can be acceptable without any agreement |

Table 11: Risk Acceptance Categories

Explicit risk estimation is used as risk acceptance principle and method is ALARP. The purpose of Risk Acceptance principle is to show that all the risks are tolerable (ALARP region) or Broadly Acceptable region. All the risks shall be reduced to ALARP, and they shall be reduced to the acceptable level (Broadly Acceptable Region).

The below figure describes the ALARP principle.



Figure 5: ALARP Principle

The risks shall be evaluated based on the ALARP principle and acceptance as follows.

|  |  |
| --- | --- |
| ALARP Region | Risk Index |
| Unacceptable | IA, IB, IC, ID, IE, IIA, IIB, IIC, IID, IIIA, IIIB, IIIC, IVA |
| Tolerable (ALARP) | IF, IIE, IIID, IVB, IVC |
| Broadly Acceptable | IIF, IIIE, IIIF, IVD, IVE, IVF |

Table 12: Risk Acceptance Criteria

### SIL Allocation

In RDSO requirements, the FNMux System shall conform to Safety Integrity Level SIL-4 as per CENELEC standards. In this FNMux system SIL allocation is based on each hazard severity, the frequency, and the mitigations; the risks are estimated to the hazards. Safety functions are derived for each identified hazard. The SIL table identifies the required SIL for the safety-related function from the THR.

|  |  |
| --- | --- |
| **Tolerable Hazard rate (THR)**  per hour and per function | Safety Integrity Level |
| 10-9 < THR < 10-8 | 4 |
| 10-8 < THR < 10-7 | 3 |
| 10-7 < THR < 10-6 | 2 |
| 10-6 < THR < 10-5 | 1 |

Table 13: SIL Allocation as per THR

THR is allocated to the random failure integrity, in case of a single safety function protecting against the hazard it holds that the quantitative safety integrity requirement (THR) is allocated completely to that safety function that protects against that hazard (TFFR). In the case of multiple independent functions protecting against the hazard and their TFFR down to the level of the last independent functions. SIL target is apportioned to each independent function.

In this FNMux, TFFR for each function has been derived by a quantitative method. The required SIL shall be determined using the following table.

|  |  |
| --- | --- |
| **TFFR [h-1]** | Safety Integrity Level |
| 10-9 < TFFR < 10-8 | 4 |
| 10-8 < TFFR < 10-7 | 3 |
| 10-7 < TFFR < 10-6 | 2 |
| 10-6 < TFFR < 10-5 | 1 |

Table 14: SIL Allocation as per TFFR

## Hazard Analysis

The purpose of hazard analysis is to undertake an identification of the system hazards, and their causes, in order to derive system requirements for reducing or controlling risks. Methods of performing a hazard analysis are introduced in the following sections.

As briefly depicted in EN50129 hazards do have a hierarchical relationship that corresponds to the hierarchical structure of the system concerned.

As also defined per EN50129, there is a hierarchical link between hazard and cause. Equally, a relation between system boundaries and subsystem boundaries exists. A hazard of a subsystem can be a cause of a hazard of a system.

Correspondingly, hazards have the same hierarchical representation. If a hazard affects more than one subsystem, interfaces to all involved subsystems are to be considered. From these interfaces usually subsystem functions and new subsystem hazards arise.

The hazard analysis records potential hazards that could occur in the system and describes the cause(s), the element concerned, and the severity level. This is done for the different operational modes, with specific cases of hazards occurring for example, when passengers are being evacuated, or outside an operational zone.

In the initiation phase of the project a preliminary hazard analysis is undertaken, its objective is to define safety critical areas to enable the system design development to proceed with safety management criteria.

The following hazard analysis shall be conducted over the system life cycle to identify the hazards associated with system design.

| SI | Safety  Analysis  Details | Project Life cycle stage | Inputs | Outputs |
| --- | --- | --- | --- | --- |
| 1. | Preliminary Hazard Analysis  (PHA) | System definition phase | Safety Plan  System context description  List of hazards  Hazard Log template | Preliminary Hazard Analysis report  Hazard log (update) |
| 2. | System Hazard Analysis (SHA) | Requirement Phase | Safety Plan  System detailed design documents  Preliminary Hazard Analysis | System Hazard Analysis report  Hazard Log (update) |
| 3. | Interface Hazard Analysis  (IHA) | Requirement Phase | Safety Plan  System Operational Context Description  Safety Requirement Specification  System Architecture Description  Sub-Systems Interface Specifications  Preliminary Hazard Analysis  System Hazard Analysis  Interfaces Hazard Analysis | System/sub-system Interface Hazard Analysis  Hazard Log (Update)  System Safety Critical Item List |
| 4. | Fault Tree Analysis  (FTA) | Design Phase | Preliminary Hazard Analysis  Safety Requirement Specification  System Hazard Analysis  System Interfaces Hazard Analysis | FTA Report  Safety Critical items list (update) |
| 5. | Operational and Support Hazard Analysis(O&SHA) | Installation Phase | Safety Plan  Safety Requirement Specification  System Operational Context Description  Installation and commissioning plans  Maintenance procedures | System Operating and Support Hazard Analysis  Hazard Log  System Safety Critical Item List |

Table 15: Hazard Analysis

### Preliminary Hazard Analysis (PHA)

The Preliminary hazard analysis should be carried out before any significant design activity begins. It requires a full high-level description of the system’s functions, construction and its interfaces to people, environment, and other systems. The PHA shall be conducted at the System definition phase of the project lifecycle. The purpose of PHA is to identify hazards, hazard mishap risk and to identify the system safety requirements. The outcome of the hazard analysis is the PHA worksheet which is available in appendix – A.



Figure 6: PHA Process

Inputs

* List of Hazards
* System concept description
* Hazard Knowledge from similar systems

Outputs

* PHA worksheet
* Hazard Log

### System Hazard Analysis (SHA)

System hazard analysis is a method for evaluating risk at system level with the focus on interfaces and safety critical functions. The SHA is a detailed study of hazards results from system integration.

Overall, the SHA:

Verifies system compliance with safety requirements contained in the system specifications and other applicable documents. Identifies hazards associated with the subsystem interfaces and system functional faults.

Assesses the risk associated with the total system design including software and specifically of the subsystem interfaces. Recommends actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

The outcome of the hazard analysis is the SHA worksheet which is available in appendix - A.



Figure 7: SHA Process

Inputs

* System Architecture description
* Safety Requirement specification
* Safety Critical function list

Outputs

* SHA worksheet
* Hazard Log update

### Interface Hazard Analysis (IHA)

The aim of Interface Hazard Analysis is to identify hazards associated with system/subsystem interfaces. The IHA analyses interfaces between system and subsystem to identify the hazards associated with it. The IHA shall be conducted at the design & implementation phase of the project lifecycle.

The outcome of the hazard analysis is the IHA worksheet which is available in the appendix A



Figure 8: IHA Process

Inputs

* System Interface specification
* System Architecture Description
* Safety Requirement specification
* Safety Critical function list

Outputs

* IHA worksheet
* Hazard Log update

### Fault Tree Analysis (FTA)

This FTA is a top-down approach. Fault tree analysis is a safety analysis technique used to determine the root causes and probability of occurrence of a specified undesired event. The FTA shall be conducted at the design & implementation phase. FTA covers both Systematic and random faults. FTA covers multiple faults effects.



Figure 9: FTA Process

Inputs

* System concept description
* System Architecture Description
* System Requirements Specification
* Safety Critical function list

Outputs

* Fault Tree Analysis reports
* Update Hazard log.

### Operation and Support Hazard Analysis (OSHA)

The aim of OSHA is to identify those hazards associated with any task that may be undertaken by operation and support personnel. The analysis will be based on operational and maintenance procedures.

The main task of the OSHA is to identify safety-critical tasks of the operation and maintenance procedures. The analysis will also identify the specific nature and duration of actions that occur under hazardous conditions during the various stages of in-service usage such as testing, installation, migration, modifications, maintenance, support, transportation, servicing and storage operation and training.

The outcome of the hazard analysis is the OSHA worksheet which is available in the appendix – A



Figure 10: OSHA Process

Inputs

* System concepts description
* System Operation
* Installation and commissioning plans
* Maintenance procedures

Outputs

* Safety requirements
* Hazard Log update
* OSHA Worksheet

### Hazard Log Management

The document in which all safety management activities, hazards identified, decisions made, and solutions adopted, are recorded. The hazard log shall be created and maintained throughout the life cycle from risk analysis phase to until the decommissioning and disposal of the system.

The hazard log shall consist of

* The aim and its purpose
* Each hazard is responsible for managing the hazard and the contributing functions or components.
* Likely consequences and frequencies of the sequence of events associated with each hazard.
* The risk arising from the consequences of each hazard (in quantitative or qualitative terms)
* Risk acceptance principles selected and in case of explicit risk estimation also the risk acceptance criteria to demonstrate the acceptability of the risk control related to the hazards.
* For each hazard: the measures taken to reduce risks to a tolerable level or to remove the risks, including evidence that the measures are effectively implemented.
* The structure of the hazard log template is shown in appendix A.
* The hazard log shall be updated, whenever a change to identified hazards occurs or a new hazard is identified, throughout the life cycle. The hazard log is dynamic and must be updated regularly, especially when.
* A relevant hazard or potential accident is identified.
* A relevant incident occurs.
* Further information emerges relating to existing hazards, incidents, or accident sequences.
* Safety documentation is created or re-issued.
* The hazard log shall be maintained.

## Handling of Systematic faults

Systematic faults are caused by human errors in the various stages of the system and subsystem of the life cycle. Following are the examples of Systematic faults.

* Specification errors
* Design errors
* Manufacturing errors
* Installation errors
* Operation errors
* Maintenance errors
* Modification errors

Systematic faults can be eliminated by means of Quality management, Safety management and technical defenses and measures.

Following are the phases to be planned to mitigate Systematic faults.

### Safety planning and quality assurance activities

It is not possible to list all individual causes of systematic faults during the life cycle phases, because systematic faults have different effects in the different life cycle phases and measures are dependent on the application. A quantitative analysis for the avoidance of faults is therefore not possible.

Following techniques to be followed as Quality assurance activities.

* Checklists
* Audit of tasks
* Inspection of issues of documentation
* Definition and review of safety plan

### Safety Requirement specification

Following checklist to be followed while preparing FNMux Safety requirements Specification.

* Graphical description, e.g. block diagrams.
* Structured specification

### Safety Organization

During the preparation of a FNMux Safety Plan the safety management structure shall be identified. Following requirements to be followed

* Training of staff in safety organization
* Independence of roles
* Qualification of staff in safety organization

### Architecture of system, subsystem

While designing FNMux System or subsystem architecture at least one of the technique or

Combination can be chosen.

* Single electronic structure based on inherent fail-safety.
* Single electronic structure based on reactive fail-safety.
* Dual electronic structure based on composite fail-safety with fail-safe comparison.
* Diverse electronic structure with fail-safe comparison

### Design Features

The below table gives techniques/measures for the avoidance and control of faults caused by

* Random events.
* Any residual design faults.
* Environmental conditions.
* Misuse or operating mistakes.
* Any residual faults in the software
* Human factors

|  |  |
| --- | --- |
| SI | Technique/Measure |
|  | Protection against operating / maintenance errors |
|  | Operator / maintainer friendliness to reduce the probability of human errors |
|  | Protection against single faults for discrete components |
|  | Protection against single faults for integrated circuits for digital electronic technology |
|  | Detection of single faults |
|  | Multiple faults |
|  | Dynamic fault detection |
|  | Retention of safe state |
|  | Program sequence monitoring |
|  | Measures against voltage breakdown, voltage variations, overvoltage, low voltage |
|  | Control of temperatures outside specified range |
|  | Software architecture and design |
|  | Protection against physical and IT-Security threats |

Table 16: Technique/Measure for Design features

### Failure and Hazard analysis Methods

In FNMux project following methods shall be used to identify and evaluate the effects of faults

|  |  |
| --- | --- |
| SI | Technique/Measure |
| 1. | Hazard and operability studies  (HAZOP) |
| 2. | Fault tree analysis |
| 3. | Common cause failure analysis |

Table 17: Failure and Hazard Analysis Methods

### Design and Development of the System, subsystem

Design method shall have the following features:

* Clear and precise documentation
* Clear and precise expression of functionality
* Transparency, modularity, and traceability
* Technological and time-related information
* Testability during verification and validation.

Following techniques/measures to be followed

|  |  |
| --- | --- |
| SI | Technique/Measure |
|  | Structured design |
|  | Graphical description including for example block diagrams |
|  | Modularization |
|  | Formal or semiformal design specification |
|  | Computer aided design tools |
|  | Environmental studies |

Table 18: Techniques for Design and development of system, subsystem

### Safety Verification and validation of the system

|  |  |
| --- | --- |
| SI | Technique/Measure |
|  | Structured design |
|  | Graphical description including for example block diagrams |
|  | Modularization |
|  | Formal or semiformal design specification |
|  | Computer aided design tools |
|  | Environmental studies |

Table 19: Techniques for Safety verification and validation of system and subsystem

### Application, operation, and maintenance

The results of the design/development phase and of the safety case will lead to

application, operation, and maintenance procedures which shall be documented considering the techniques/measures provided in the table below.

|  |  |
| --- | --- |
| SI | Technique/Measure |
|  | Production of applications operational and maintenance manuals and instructions |
|  | Training in the execution of operational and maintenance instructions |
|  | Maintenance friendliness |
|  | Protection against physical threats |
|  | Protection against IT Security threats |

Table 20: Techniques for Safety verification and validation of system and subsystem

## Safety Review and Audits

* The periodic reviews & audits shall be conducted by the Safety Team during the life cycle of the system.
* The team shall review the system performance by analysing the failure reports from the field.
* The team shall identify the critical and catastrophic errors from the performance report.
* Make a hazard log entry for the failures of the following category.
* Failures which cause severe loss of the system, damage of the equipment or person.
* Failure, which is occurring repeatedly irrespective of the railway zone, site, & environment etc.
* The team shall recommend the mitigation requirements for the intolerable & undesirable risks to design team to reduce the level of risk associated with the system failures.
* The Safety team shall review the design changes made to reduce the risk level and generate a risk acceptance report.
* The Safety plan shall be reviewed and updated from the necessary phase of the lifecycle based on the modifications to the system design.
* The Safety review shall be conducted during the changes in the existing design, design modification in the specific application due to requirement changes or due to any other reason.
* The Safety review shall be conducted by a team of safety engineer/experts headed by System Manager.
* The review report shall be documented and further safety process for the changes shall be discussed in the review report.
* Based on the design changes, the suitable life cycle phase shall be identified and discussed with proper justification in the safety review report.
* The audit is a safety assessment process conducted at appropriate stages of the life cycle.
* The audit shall be performed to assess the fulfilment of the CENELEC requirements and to confirm the guidelines of the safety standards has been properly adopted for the project.
* The Safety manager shall be responsible to conduct the audit with a suitable person who has not involved in the any kind of design activity.

## Safety Analysis of System Maintenance, Performance and Operation

For Safety analysis of FNMux system in field FRACAS process can be used. FRACAS is a process of failure reporting, analysis and corrective action system that gives organizations a way to report, classify and analyze failures, as well as plan corrective reactions in response to those failures.

A FRACAS is a closed-loop process containing the following steps:

Failure reporting (FR): All failures and faults related to a system, piece of equipment or process are formally reported using a standard form known as a failure report or defect report. The failure report should clearly identify the failed asset, symptoms of the failure, testing conditions, operating conditions, and failure time.

Analysis (A): Perform a root cause analysis to identify what caused the failure. Perform a root cause analysis to identify what caused the failure.

Corrective actions (CA): Once the cause of the failure is determined, implement, and verify corrective (or preventive) actions to prevent future occurrences of the failure. Any changes should be formally documented to ensure standardization.

## Interface with other related programme or plans

The specific safety requirements for FNMux system, subsystem including requirements for safety functions and associated safety integrity requirements, are identified, and documented in the safety requirements specification. This is achieved by means of:

* Hazard Identification and Analysis,
* Risk Assessment,
* Allocation of Safety Integrity Levels, Safety requirements derived from various Hazard analysis techniques like PHA, SHA, IHA etc shall be documented in Safety requirements specification document.

# Safety case

## Safety Case Structure

The Structure of the safety case is shown below.



Figure 11: Safety Case Structure

1. Introduction

* Aim of the document
* Fields of application
* Structure of the document
* Regulations applicable to the system

1. Definition of system

* Definition of the system

1. Quality management report

* Quality plan
* Technical inspection report
* Quality testing report

1. Safety management report

* Introduction
* Safety life cycle
* Safety organization
* Safety plan
* Hazard log
* Safety requirements specification
* System design
* Safety reviews
* Verification and Validation plan
* Safety assurance
* Approval of the system by the railway authority
* Operation and maintenance
* Decommissioning and disposal
* Software development plan
* Configuration management plan

1. Technical safety report

* Introduction
* Assurance of correct functional operation
* Effects of Faults
* Operation with External Influences
* Application Conditions Affecting Safety
* System Qualification Test

1. Related Safety Case
2. Conclusions

* Summary of system operation and characteristics

1. Documents and applicable regulations

* Applicable regulations.
* RDSO input documents.
* Supplier documents required for this plan.
* Definitions, acronyms, abbreviations.

1. Appendices
2. References

## Management of SRAC

The safety related application condition is a part of the technical safety report which discusses the rules, conditions, and constraints relevant to functional safety which need to be observed in the application of the FNMux system and subsystem.

In particular, the Safety Related Application Conditions (SRAC) describes the following points to be considered for FNMux System.

* Configuration of programmable systems to suit specific applications.
* Rules and methods for maintenance and fault finding.
* Precautions in manufacturing, installation, and testing.
* Instruction for system operation.
* Safety warning and precautions.
* Electromagnetic compatibility (EMC) precautions.
* Information concerning modifications and eventual de-commissioning.
* Safety justification of support tools and equipment.
* Versions compatibility for Software and Configuration Data.

## System configuration and System build

FNMux System, subsystem needs to be configured for each application, then any configuration tools and/or procedures shall be defined.

Configuration aspects:

* Procedural methods
* Version control
* Hardware requirements of configuration system
* Software details of configuration system
* Software maintenance
* Simulation
* Configuration data specification (interface between the configurable data and the system)
* Version of configuration data.

System builds:

* Version control settings
* Application control settings
* Interface settings
* Initialization settings
* Maintenance control settings
* Manufacturing and production testing
* System test routines
* Installation, testing and commissioning.
* Data configuration tool required for system build.
* Data configuration tool version required for system build.

### SRACs for operation, maintenance, and safety monitoring

The technical safety precautions and procedures to operate and maintain the FNMux system, subsystem shall be extracted from the Operation and Maintenance Plan and documented, which shall include the following aspects:

#### Operational status

The conditions that exist in FNMux system, subsystem shall be defined to provide operating and maintenance personnel sufficient understanding during the following situations.

1. Start up:

This shall describe the start-up conditions of the FNMux system, subsystem when power is initially applied, or following shut-down due to power interruption or other cause.

* Default conditions.
* Initialization period.
* Self-checks performed.
* Manual intervention required.
* Condition of outputs.
* Precautions after an exceptional event, such as fire or unauthorized entry.

1. Normal operation:

Once the FNMux system, subsystems have successfully completed initialization, the conditions during normal operation shall be defined.

* Cycle times.
* Non data routines
* Disclosure of faults

1. Change over:

The FNMux system subsystem has a facility to change over to hot standby, then the conditions defined in a) and b) shall be re-stated for this changeover routine. The reaction of the system to the changing of failed modules shall also be clearly defined.

1. Shutdown:

When a Kavach system, subsystem is shut down intentionally for a configuration change or de-commissioning, or unintentionally via a power failure, then all relevant conditions shall be defined.

* Default conditions.
* Conditions for graceful degradation.
* Safety aspects.
* Procedures.
* Influences on other connected systems.

#### Maintenance levels

These shall be defined with respect to:

* First line maintenance by the maintainer (Preventive maintenance and fault-finding/repair carried out on site)
* Second line maintenance by the maintainer (Preventive maintenance and possible repair in a workshop environment)
* Second line maintenance by supplier

#### Periodic Maintenance

In describing the periodic maintenance required, reference shall be made to all relevant areas.

* Training
* Accessibility
* Modularity
* Interchangeability
* Spares provision.
* Storage of spares.

#### Maintenance Aids

For each level of maintenance of FNMux system, subsystem, the maintenance aids available to personnel shall be defined. This aid can be included.

* Fault diagnostic
* Interpretation of fault messages

### SRACs for decommissioning and disposal

The technical safety precautions and procedures which will be necessary when the FNMux system, subsystem is eventually decommissioned shall be documented here. This shall include consideration of possible phased introduction of replacement systems whilst the railway continues in operation. Appropriate warnings and instructions concerning the final disposal of FNMux equipment after decommissioning shall also be included.

# Safety Assessment and authorisation Process

## Safety Assessment Process

The Independent safety Assessment for FNMux shall be conducted by M/s. BV (Assessor), a member of the RDSO ISA panel list.

The Independent Safety Assessor performs the following assessment activities for FNMux:

* Brief Review of the product under assessment / certification.
* Preparation of an Assessment Plan.
* Perform necessary Document Review, Quality & Safety Audit of the organization, review skill and competency of the person involved and compliance verification to establish conformity of the FNMux, for adequacy to the RDSO specifications and in line with CENELEC.
* 1st analysis of documentation for the identification of documents for Assessor review.
* Review of the documents over 2 review cycles, i.e., issue of comments on the 1stsubmission through a comment resolution sheet and review of 2nd submission for satisfactory compliance.
* The functional audit is performed on products including system & software and V&V reports. i.e., Documental set will be analyzed on completeness, validity, not ambiguity, comprehensibility, and consistency against CENELEC Standards.
* Issue of intermediate review report (technical note on the document analyzed) and final review report, after satisfactory closure of all open points.
* The final review evaluation report is a summary of technical Notes and is based on life cycle applied by manufacturer according to quality and safety regarding CENELEC principles and will consider evidence of Quality/Safety Management activities.
* Concerning the quality management, following main topics will be examined:
* Quality Planning/Reporting
* Quality Certificate
* Training
* Proof of competence
* Configuration Management / archiving
* Final safety case
* Concerning the quality, the Safety Management activities applied product the following main topics will be examined:
* Lifecycle (Plans)
* Roles and Responsibilities – Independence (Plans)
* System Definition
* Risk Analysis / Hazard Control
* System Safety (Requirements Management)
* Apportionment of Requirements
* Validation
* System Acceptance
* Inspection and witness functional tests of the products in test lab / field as necessary.
* Issue of final summary of the technical Notes, based on the life cycle, applied by manufacturer, according to quality and safety CENELEC principles, considering the evidence of Quality/Safety Management activities.
* The safety assessor shall issue an intermediate and final safety assessment report followed by a certificate of compliance.

## Safety Authorisation Process

RDSO is authorization body for FNMux equipment, following set of activities shall be performed to get approval with RDSO.

* Registration with RDSO for FNMux development.
* Quality assessment by RDSO.
* Engagement of ISA to FNMux life cycle.
* Design of the System.
* Demonstrate the functionality to RDSO.
* Demonstrate the quality and technical safety to ISA.
* Conduct Reliability testing (Type testing).
* Field trial.
* Demonstrate System Safety to ISA.
* Certificate of Compliance by ISA.
* System Approval by RDSO.

### Registration with RDSO for FNMux development

TE shall register the firm for development of the FNMux system as per ISO 9000:2015.

### Quality Assessment by RDSO

After the firm applied for registration, RDSO will assess the quality and ability of the firm for executing the project. RDSO follows the ISO 9000:2015 standard for quality assessment of the firm.

### Engagement of ISA to FNMux life cycle

After quality assessment of RDSO, TE shall engage an ISA for FNMux system, from the approved ISA list of RDSO, The ISA is responsible for assessment of FNMux system.

### Design of the System

TE shall design and develop the FNMux system as per CENELEC standards EN50128, EN50129, EN50126.

### Demonstrate the functionality to RDSO

After design and development is completed, the FNMux system shall be tested by IV &V team for fulfillment of all RDSO requirements, Reliability and Safety requirements. After complete system testing by IV & V, TE shall demonstrate the FNMux System functionality to RDSO in lab premises and get approval for initial field trials.

### Demonstrate the Quality and Technical Safety to ISA

TE shall demonstrate the quality of the system as per ISO 9001 standard and technical safety as per EN50128, EN50129 and EN50126 to ISA. ISA shall issue an intermediate safety assessment report.

### Conduct Reliability Testing

After functional testing by RDSO, TE shall conduct FNMux system Type testing/ Reliability testing in RDSO lab or any approved labs as per FNMux RDSO specification.

### Field trial

FNMux field trials to be performed for checking system performance in field. Parallel, series and standalone trails shall be performed as per RDSO guidelines. The Parallel, series and standalone field trial period shall be decided by RDSO.

### Demonstrate System Safety to ISA

ISA shall test FNMux system in the lab and field for its Safety acceptance.

### Certificate of compliance by ISA

ISA Issues certificate of compliance, based on the life cycle, applied by manufacturer, according to quality and safety CENELEC principles, considering the evidence of Quality/Safety Management activities.

### System approval by RDSO

Firm shall submit field trail reports to RDSO, after successful completion of field trial firm shall request for initial type approval to RDSO with formal letters. RDSO issues initial type approval after examining field trail reports.

# Safety Life Cycle Deliverables

The following safety deliverables shall be produced for the Kavach.

|  |  |
| --- | --- |
| SI | Deliverables |
|  | Safety Plan |
|  | System Safety Requirements Specification |
|  | Preliminary Hazard Analysis (PHA) |
|  | System Hazard Analysis (SHA) |
|  | Interface Hazard Analysis (IHA) |
|  | Operational & Support Hazard Analysis (OSHA) |
|  | Fault Tree Analysis (FTA) |
|  | Hazard Log |
|  | Safety Verification Report |
|  | Safety Case |

Table 21: Safety Deliverables

# Appendix A: Hazard Analysis Templates

The Hazard Analysis templates used for the project are defined below.

## Preliminary Hazard Analysis

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hazard Identification | | Failure Identification | | | Initial Risk evaluation | | | Failure Management | | | **Comments** |
| PHA ID | Hazard | Causes | Phase | Potential Accident | Severity | Frequency | Risk Assessment | Mitigation  Req. ID | Mitigation Measure | Mitigation Owner |

Table 22: Preliminary Hazard Analysis

## System Hazard Analysis

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hazard Identification | | | Failure Identification | | | | Initial Risk evaluation | | | Failure Management | | Comments |
| SHA ID | System Function | Hazard | Operating Mode | Potential Accident | Cause | Effect | Severity | Frequency | Risk Assessment | Mitigation Measure | Mitigation Owner |

Table 23: System Hazard Analysis

## Interface Hazard Analysis

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hazard Identification | | Failure Identification | | | | Initial Risk evaluation | | | Failure Management | | Comments |
| IHA ID | Hazard | Failure Mode | Effect | Cause | Potential Accident | Severity | Frequency | Risk Assessment | Mitigation Measure | Mitigation Owner |

Table 24: Interface Hazard Analysis

## Operating & Support Hazard Analysis

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hazard Identification | | Failure Identification | | | | Initial Risk evaluation | | | Failure Management | | | Comments |
| OSHA ID | Hazard | Failure Mode | Effect | Cause | Potential Accident | Severity | Frequency | Risk Assessment | | Mitigation Measure | Mitigation Owner |

Table 25: Operating & Support Hazard Analysis

## Hazard Log

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hazard Identification | | Failure Identification | | Initial Risk evaluation | | | Failure Management | | Final Risk Evaluation | | | **Evidence Link** | **Status** | **Comments** |
| Hazard ID | Potential Hazard | Hazard cause | Potential Accident | Severity | Frequency | Risk Assessment | Mitigation Measure | Mitigation Owner | Severity | Frequency | Risk Assessment |

Table 26: Hazard Log