1 DEFINITION OF THE PROJECT SYSTEM

<This section shall present a description of the system as required by the EN 50129 standard **Error! Reference source not found.**. For a more detailed system description the reader should refer to Requirements Specification [Ref], Interface Requirements Specification [Ref] and Architecture Specification [Ref].>

1.1 PROJECT SYSTEM DESCRIPTION

<This section shall provide a few pages with the description of the system under certification, focusing on the generic application details. Description of the system components, new subsections can and shall be added to ease the readability. One or more images and schemas shall be used to show the relation and interfaces between the components/subsystems. An overview of the functional objective and the safety level of the system shall also be provided.>

<The description of the system, would include at least:

- System interfaces & interface elements
- Description of system functional and safety functions
- System functional and safety states
- System operational context diagram
- System context elements
- System use cases
- Possible system configurations

Sub sections for the above topics may be created if they enable a better understanding of the system.

The system overview section enables the reader to have a quick view about the system and what it does.>

1.2 PROJECT INTERFACES

<This section shall describe the system interfaces with the help of diagrams and figures, supported by explanation text.>

1.3 PROJECT FUNCTIONS

<This section shall describe the system functions (by main groups or hierarchy, including the data preparation system) with the help of diagrams and figures, supported by explanation text.>

1.4 PROJECT STATES

<This section shall describe the system states with the help of diagrams and figures, supported by explanation text.>

1.5 PROJECT HARDWARE ARCHITECTURE

<This section shall describe the hardware architecture with the help of diagrams and figures, supported by explanation text. The redundancy strategy, interconnections, hardware systems layouts must all be described in this section.>

1.6 PROJECT SAFETY FUNCTIONS

<This section shall describe the system safety functions, particularly as stated in EN 50129 **Error! Reference source not found.**, safety functional requirements and safety integrity requirements. Diagrams, tables and figures, supported by explanation text shall be provided. SIL allocation shall also be provided, even for the hardware components.>

1.7 SYSTEM CHARACTERISTICS

<This section shall describe the system characteristics with the help of diagrams and figures, supported by explanation text. It is important to refer to other documents with more details.>

1.8 SYSTEM PERFORMANCES

<This section shall describe the system performances with the help of diagrams and figures, supported by explanation text. It is important to refer to other documents with more details. It is important to consider the communication subsystems, data management tools, redundancy impacts, system inputs impacts, system outputs impacts, error detection influence, event and error storage capacities, etc.>

1.9 SYSTEM CONFIGURATION

<This section shall list and describe the components that constitute the system (hardware, software and application data) and their versions (configuration).>

1.10 DOCUMENTATION DEFINITION AND MANAGEMENT

<This section shall list and describe the documentation at system/generic application level, in principle references to the Configuration Management Plan [Ref] should be enough for the documentation

description and management, thus this section can contain an overview of the documentation control and configuration, especially for the product documentation.

The section shall describe also the documentation traceability management, tools and processes, in particular the documentation change processes.

The documentation management including configuration control, documentation issue tracking, and usage of tools must also be described or referred.>

2 QUALITY MANAGEMENT REPORT

<This section shall (as stated in EN 50129 **Error! Reference source not found.**) present the generic application quality management report.

This section shall demonstrate the quality processes and procedures that the application is compliant with and reference them above in the references section.

The purpose of the applicable quality management system is to minimize the incidence of human errors at each stage in the life-cycle, and thus to reduce the risk of systematic faults in the system, sub-system or equipment.

Running quality certifications related to quality and safety shall be mentioned and referred to in this section.

Therefore, this second part of the Generic Application Safety Case shall be implemented in accordance with the applicable standards to the system presented in the previous section (Refer applicable standards such as EN ISO 9001:2008, EN ISO 9000:2005, EN ISO 9004:2009, EN ISO 90003:2004, ISO/IEC 9126, ISO 25000, etc. and reference them above in the references section).>

2.1 QUALITY ORGANISATION

<This section shall present the high level organisation (a figure), roles and main activities, then the detailed project organisation (figure), roles and main activities. Particular attention should be given to the Safety/RAM and Validation teams.>

2.1.1 Personnel Competences

<According with EN 50126 **Error! Reference source not found.** all personnel involved in the development of the system shall have previous experience in the domain and enough competences for the project development.

The competence evidences for the main key persons of the project shall be presented (e.g. present the list of personnel involved in the application development or refer to Project Management Plan [Ref]).

2.2 QUALITY ACTIVITIES

<The quality activities executed in the project shall be detailed in several plans, the more important and applicable for this section is the Quality Plan [Ref]. The next sections shall present the different plans used as a basis for the quality assurance of the entire system/product development.>

2.2.1 Project Plan

Make a reference to the generic project plan and highlight the main work-packages.

2.2.2 Quality Plan

Make a reference to the Quality Plan and provide a summary and the main activities of the plan.

2.2.3 Safety Plan

Make a reference to the safety plan and highlight the main safety-related activities.

2.2.4 Verification Plan

Make a reference to the verification plan and highlight the main verification activities.

2.2.5 Validation Plan

Make a reference to the validation plan and highlight the main validation activities.

2.2.6 RAM Plan

Make a reference to the RAM plan and highlight the main RAM activities.

2.2.7 Configuration Management Plan

Make a reference to the CM plan and highlight the main CM activities and processes.

2.2.8 Software Quality Assurance Plan

Make a reference to the SQAP and highlight the main software quality assurance techniques and methods.

2.2.9 User and Maintenance Manual

Make a reference to the User and the Maintenance manuals and highlight the main related processes.

2.2.10 System and Interfaces Definition

Make a reference to Section 2 where the system and its interfaces is already described and provide links or overview of Requirements Specification [Ref], Interface Requirements Specification [Ref] and Architecture Specification [Ref] related to system interfaces.

2.3 QUALITY EVIDENCES

<The quality evidences for the application must be presented throughout the different documents produced along the development cycle. The next sections shall provide a summary of these documents.>

2.3.1 EN 50129 to Project Process Traceability

In order to demonstrate compliance between the project Quality Plan and the requirements presented in EN 50129 **Error! Reference source not found.** a traceability table shall be presented, including the EN 50129 requirements and the Quality Plan section.

2.3.2 Quality Documentation

This section shall list the documents produced during the application development related to quality management activities (e.g. review reports, verification reports, change requests, validation reports, etc.).

2.4 QUALITY CONTROL

<This section shall provide a summary of the quality control activities – see examples hereafter.>

2.4.1 Audits

The quality audits allow having a systematic and independent examination that checks if the necessary quality documents are being produced in accordance with the defined processes and project plans.

All the produced documents shall be clear and consistent along the development life cycle, centred in the evidence and compliant with the phase requirements.

Provide or refer to a complete list of audit reports.

2.4.2 Reviews

Short description of the reviews activities. Refer to the different types of reviews: Requirements, Design and Source Code reviews, Informal reviews, Safety Plan Reviews, etc.

3 SAFETY MANAGEMENT REPORT

<This section shall describe the Safety Management process used during the development cycle of the generic application.>

3.1 INTRODUCTION

<Provide a short introduction, e.g.:

This section takes into consideration the requirements presented in the EN 50129 **Error! Reference source not found.** to obtain the system approval by the certification authority.

The main objective of the safety management procedure is to provide a systematic process to reduce the rate of human induced errors during the product lifecycle and also to minimize the probability of systematic errors during the application operation period.

The Safety Plan **Error! Reference source not found.** presents in detail each one of the activities and documents necessary to achieve the desired level of safety management. The Validation Plan [Ref] presents the activities and methods used to validate that the system is able to operate with the necessary safety assurance during the life cycle.>

3.2 SAFETY LIFECYCLE

<Describe and refer to the applied safety lifecycle, namely as reported in the Safety Plan **Error! Reference source not found.** and the Validation Plan [Ref] and the standards EN 50129 **Error! Reference source not found.** and EN 50126 **Error! Reference source not found.**.>

3.3 SAFETY ORGANISATION

<Depict and describe the safety related team roles and responsibilities as a continuation of the organization description provided in section 3. Highlight the independence principle as required by EN 50128 **Error! Reference source not found.**.>

3.4 SAFETY PLAN

<This section shall refer to the Safety Plan **Error! Reference source not found.** and provide an overview of the safety management processes. It shall be compliant to section 5.3.4 of the EN 50129 **Error! Reference source not found.** standard.>

3.5 Hazard Log

<The Hazard Log **Error! Reference source not found.** shall be referred and an overview provided in this section, that shall comply with section 5.3.5 of EN 50129 **Error! Reference source not found.**. The hazards management as stated in the Safety Plan **Error! Reference source not found.** shall also be referred>

3.6 Safety Requirements Specification

<The safety requirements specification shall be elaborated during the system lifecycle, namely during the Preliminary Hazard Analysis and Hazard Analysis activities of the development lifecycle. Provide here a reference to these reports, the specification, the validation plan and how these requirements are managed and updated. This section shall comply with section 5.3.6 of EN 50129 **Error! Reference source not found.**.>

3.7 System Design

<The system design shall be performed after defining the system requirements and safety requirements. The system must be built based on the performance that it needs to achieve, and also taking into consideration the safety targets applicable to the system. This section shall present a simple view of the main flows of the system design process and shall comply with section 5.3.6 of EN 50129 **Error! Reference source not found.**.>

3.8 Safety Review

<Refer to the documents that contain the safety reviews, especially the Safety Plan **Error! Reference source not found.** and the Validation Report [Ref] and provide a short overview. Include, at least, the system requirements to system architecture traceability matrix, the system architecture to the software traceability matrix, the system architecture to the hardware traceability matrix, the system architecture to the integration test traceability matrix, the system requirements to the validation test traceability matrix.>

3.9 Validation Plan

<Refer to the Validation Plan [Ref] and provide a short overview of its contents, giving focus to the safety requirements validation and the independence principle.>

3.10 Safety Assurance

<The safety assurance of application development must be confirmed by the entire safety management process (described in this section and detailed in the Safety Plan **Error! Reference source**

not found.) and also the validation reports, including the technical and functional assurance described later in this document (section 5).

The Safety Case (this document) is the ultimate evidence of safety assurance for the project, demonstrating that the EN 50129 **Error! Reference source not found.** standard requirements are accomplished.>

3.11 Acceptance of the System

<The acceptance of the system by the Railway Safety Authority will take place after the demonstration of the system full compliance with the functional and safety requirements specified for the system.

The compliance with those requirements is demonstrated in the present document, with special emphasis on section 5 where it is demonstrated if all the safety requirements were implemented and validated.

Sections 3 and 4 present, respectively, the Quality Management and the Safety Management processes applied to the application development.>

3.12 Operation and Maintenance

<The operation and maintenance activities of the generic application must be detailed in the User and Maintenance Manual [Ref].

If, during operation, any modification to the system is necessary, the impact of the specific modification need to be analysed and evaluated in order to quantify the impact on the system, and especially in the safety part of the system. In case of changes that affect system safety, the Hazard Log **Error! Reference source not found.** shall be updated and if necessary new safety requirements issued or updated.>

3.13 Decommissioning

<The decommissioning activity related to the generic application shall be described in this safety case.

The decommissioning of the system is the last phase of the lifecycle, accordingly with EN 50126 **Error! Reference source not found.** generic lifecycle, therefore the generic application is able to present only a part of the overall decommissioning procedure and these particular provisions, that affect the final decommissioning activities of the system, shall be described here.>

4 TECHNICAL SAFETY REPORT

<This section shall describe the Technical Safety demonstration according the requirements of EN 50129 **Error! Reference source not found.**.>

4.1 INTRODUCTION

<Provide a short introduction, e.g.:

The technical safety demonstration shall be able to show that the system is safe. It is also able to detect deviations from the normal course of operations, i.e. detects errors or faults that can cause deviations from the nominal way of work.

In case an error is detected the system shall be able to maintain the safe state on the railway environment, using for that all the necessary means of operation to go into the safe state and to maintain the railway system on it until the deviation is corrected.

The next sections provide the necessary details for the safety demonstration of the system (generic application). Several references to external documents are provided in order to reduce the details in the present document. Whenever necessary an explanation of the method or technique used to accomplish a certain objective is presented.>

4.2 ASSURANCE OF CORRECT FUNCTIONAL OPERATION

<This section shall provide the necessary evidences to demonstrate the correct operation of the application with a nominal environment, i.e. without faults.

In case of a fault-free environment the application shall be able to maintain its operation within the specified parameters. The next sections shall present some aspects of the application that are relevant for the technical safety demonstration of correct functional operation.

In this case the system is considered as the generic application.>

1. System Architecture Description

Refer to the section of the System Architecture and other relevant documents.

2. System Interfaces Definition

This section shall describe the system interfaces. The interfaces that can be causes for safety issues shall be more detailed, as well as MMI and internal and external interfaces between the system and other systems.

3. System Requirements Specification Fulfilment

The compliance with the System Requirements Specification [Ref] regarding functional, interface and performance requirements shall be accomplished by the design and implementation of the system itself. Evidences for compliance are achieved by system verification and system validation. These independent ways must be described in this section and subsequent sub-sections (by specifying the activities per lifecycle).

4. Safety Requirements Specification Fulfilment

The same activities as in the previous section shall apply.

Additionally, a safety analysis must be performed over the system implementation to see if any new hazards appear during the implementation phase.

The safety analysis is part of the Hazard Analysis document [Ref] and all the findings are reported in the same document and in the Hazard Log [Ref].

An independent section in the Safety Validation Report [Ref] shall be used to demonstrate the safety requirements conformance.

With the complete set of verifications, safety analysis and validations it must be possible to demonstrate that the safety requirements are fulfilled by the system implementation and that no hazardous situation are expected to occur.

5. Correct Hardware Functionality Assurance

The system hardware parts shall be described in section 2.

In order to assure the correct hardware functionality a series of analysis must be performed over each of the hardware items that compose the generic application.

The RAM analysis of the system is specified in the RAM Plan [Ref] and the detailed results are presented in the RAM Report [Ref].

This section shall provide and justify the hardware components reliability values, availability percentages, Maintainability values and safety strategies (based on the Hazard Analysis).

6. Correct Software Functionality Assurance

In order to ensure the correct functioning of the software in the generic application a set of verification and validation activities must be executed according to the software development process defined for the project, referring the verification and validation plans, and in conformance with the EN 50128 standard **Error! Reference source not found.**.

This section should contain several sub-sections to present the software for the application, including a description of the development process, namely: Software Architecture, Software Interfaces, Software Behaviour to comply with the system architecture, Response Times, Software Behaviour in the Event of Hardware Failures, Development Process detailed containing all the lifecycle phases and relevant activities, communication protocols analysis (if applicable), network security (if applicable), etc.

7. Data Preparation Process

Detail the data preparation process for the configuration of the generic application (and later specific application) that shall be based on a set of activities focused in the following:

- Data from customer (system definition, including rules and schematics for the deployment location);
- Software tools (configuration and validation tools);
- Validity check (in field tests);
- Reports on the executed activities.

The data/application preparation process shall be referred and an overview shall be provided in this section containing at least the process definition, activities, roles and responsibilities.

4.3 EFFECTS OF FAULTS

<This section shall provide the strategy and design approaches to assure a safe response in case of faults. The system must be designed and developed in order to react, thanks to safety techniques, in a safely manner in the presence of one or more single random failures and in order to avoid wrong side systematic errors thanks to additional and dedicated analysis.

In accordance with the standard EN 50126 **Error! Reference source not found.** a Preliminary Hazard Analysis (PHA) [Ref], and a Hazard Analysis (HA) [Ref] of the generic product must be performed. A list of potential hazards that can occur in the railway system where the generic product can be deployed is also necessary, indicating the hazards that can be mitigated by the system itself and the hazards that need to be mitigated by another component of the railway system. This list is contained in the Hazard Log [Ref].

The different topics that could be described in this section include:

- Effects of single Faults;
- Independence of Items;
- Detection of Single Faults;
- Actions Following Detection;
- Multiple Faults;
- Protection against operating errors and sabotage;>

4.4 Operation with External Influences

<This section shall provide the generic application operations that are foreseen for operations and external communications, if applicable. This can include protection against unauthorized access and tests with severe conditions.>

4.5 Safety Related Application Conditions

<This section shall present the safety-related application conditions required in order to maintain the system safety. The necessary safety related application conditions for the Generic Application shall be presented here (these are also presented in the Hazard Log document for reference **Error! Reference source not found.**).

The System Configuration and Manufacturing, including the operational state, periodic maintenance and tools needed for maintenance operations shall also be described.

The Operational Safety Monitoring activities and the decommissioning and disposal activities must also be referred, taking into account the contribution of the generic application.>

4.6 Safety Qualification Tests

<Describe the complete set of safety qualification tests executed at this level (Generic Application)assuming that the system is being developed as a generic product.

The safety tests are expected to be executed, specified in the Safety Validation Test Specification [Ref] and the results presented in the Safety Validation Report [Ref].

According to the results presented in the Safety Validation Report [Ref], all the safety qualification tests must be positive in the actual version of the application, and also for the Generic Product (as a pre-requisite).>

5 RELATIONSHIPS WITH OTHER SAFETY CASES

<This part of the Safety Case document shall refer to the related safety cases.>

5.1 Related Safety Cases

List and described the other existing safety cases that are related to this one. Make a more detailed description for each of them in a sub-section and present theirs SRACs.

8. Generic Product Safety Case

This safety case shall be the direct instantiation of the Generic Product Safety Case for the Generic Application.

9. Safety Case 2

6 SAFETY CASE CONCLUSIONS

<This section shall present a summary of the present safety case and the final safety statement for acceptance of the system generic application.>

6.1 SUMMARY

State that this safety case intends to provide evidences to prove that all necessary conditions for compliance with the CENELEC standards and related SIL X are met. Provide an overview with one paragraph for each section and the relevant evidences (sections 3, 4 and 5).

6.2 FINAL STATEMENT

Refer to any limitation or open points.

Provide a statement such as:

The final positive safety conclusions declare that the Release/version xxxx of the generic application is useful for revenue service.