ENG-RSC-EN-RR-DTRF-0001

C

# DTRF 150801 Generic Safety Specification for Supplied Sub-System

## DOCUMENT SUMMARY :

DTRF 150801 version 1 (doc base KM Metiers)
Previous reference ENG-RSC-EN-RR-PRO-0002
Modification requested by Raoul ROLAND on May 2020

| Design Office | APPLICATIONS (Series of Rolling Stock or application) | N$^{er}$ of assembly drawings |
|---|---|---|
| | Railway Rolling Stock | |
| | | |

# *TECHNICAL SPECIFICATION*

# Generic Safety Specification for Supplied Sub-System

| | | Date | Name | |
|---|---|---|---|---|
| | Written by | | P. Cozzarin | |
| | Reviewed | | R. Roland | |
| Manufacturer's modifications | Approved | | R. Roland | ALSTOM Version : English |

| | |
|---|---|
| 0 | 06/07/2015 |
| 1 | 07/2017 |
| C | 03/2021 |

Gen. Spec..

**Generic Safety Specification for Supplied Sub-System**

Replaces

Page 1 / 23 Pages

| | Date | Name |
|---|---|---|
| | | |
| Verified | | |
| Homol. | | |

Format

**ENG-RSC-EN-RR-DTRF-0001 DTRF 150801**

# Revision records table

| Index | Date | Description of change | Name |
|---|---|---|---|
| 0 | 06/07/2015 | First issue | C. Schor |
| 1 | 07/2017 | Update from feedback of exchanges with suppliers<br>Addition of Coupler and Brakes generic failure modes and default planning for deliverables. | R. Roland |
| C | 03/2021 | Update from feedback of exchanges with suppliers<br>Addition of Toilet, Master Controller and Fire Detection generic failures | Ph. Cozzarin |

ALSTOM

# CONTENTS


1 PURPOSE ..... 4
2 TERMS AND DEFINITIONS ..... 4
3 APPLICABLE STANDARDS ..... 4
4 SAFETY MANAGEMENT ..... 5
4.1 LIST OF TYPICAL DOCUMENT AND SAFETY ANALYSES ..... 5
4.1.1 SAFETY PLAN ..... 5
4.1.2 HAZARD ANALYSIS ..... 5
4.1.3 FMEA / FMECA ..... 6
4.1.4 FAULT TREE (SAFETY) ..... 6
4.1.5 SAFETY MANAGEMENT FILE ..... 6
4.2 ACTIVITIES BEFORE THE CONTRACT SIGNATURE ..... 7
4.3 ACTIVITIES DURING DEVELOPMENT PHASE ..... 8
4.4 ACTIVITIES DURING THE OPERATION PHASE ..... 9
5 TYPICAL SAFETY REQUIREMENTS ..... 9
5.1 HVAC ..... 10
5.2 PANTOGRAPH ..... 11
5.3 DOORS ..... 12
5.4 AUXILIARY BATTERY ..... 13
5.5 COUPLER ..... 14
5.6 BRAKES ..... 16
5.7 FIRE & SMOKE DETECTION (AND EXTINGUISHING) SYSTEM (FSD) ..... 18
5.8 MASTER CONTROLLER (MC) ..... 19
5.9 TOILET ..... 20
5.10 OTHER COMMODITIES ..... 21
6 SAFETY DELIVERABLES ..... 22

# 1 PURPOSE

The purpose of this document is to describe the management requirements and the generic requirements related to Railway Safety.

# 2 TERMS AND DEFINITIONS

| Terms | Definition |
|---|---|
| CGR | Critical Gate Review |
| FAI | First Article Inspection |
| FSD | Fire & Smoke Detection |
| MC | Master Controller |
| PGR | Preliminary Gate Review |
| SGR | Specification Gate Review |
| SIL | Safety Integrated Level. |
| SRAC | Safety Related Application Conditions |
| SSIL | Software Safety Integrated Level. |

# 3 APPLICABLE STANDARDS

| References | Observation |
|---|---|
| EN50126-1:2017 | Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part1: Generic RAMS Process |
| EN50126-2:2017 | Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part2: Systems Approach to Safety |

# 4 SAFETY MANAGEMENT

The Supplier agrees to:

- Supply a safe product,
- Comply with EN50126 part 1 and 2 and the regulations applicable to the project,
- Justify that the product satisfies specified safety requirements,
- Be fully responsible for the performances of his system.
- Inform Alstom about Safety Related Application Conditions (SRAC) and assumptions for which it is not responsible (related to storage, operation, inspection, etc.).

The Supplier shall assist Alstom until the supplied product has been approved. It shall answer questions and comments made by Notified/Designated Body (NoBo/DeBo) and Independent Safety Assessor (ISA) if any and shall provide all requested studies and demonstrations.

## 4.1 LIST OF TYPICAL DOCUMENT AND SAFETY ANALYSES

The following documents are typical safety deliverables and these analyses will be carried out by the supplier (depending on project and product specificities, see §6 for details) and justify that the commitment on safety objectives will be achieved.

Complementarily any specific requirements will be addressed in TPS.

### 4.1.1 SAFETY PLAN

The Safety Plan is the set of Safety activities in accordance with the Safety Management System of the supplier that are applied throughout the product lifecycle to ensure that the Subsystems delivered to Alstom is safe and remains safe up to dismantlement.

The purpose of a Safety Plan is to define the Safety requirements of the subsystem and the methods by which the safety level will be assessed and managed. This will detail resources, processes and safety management activities. It will be subject to on-going audit and verification and will contain clear safety objectives and deliverables. All safety deliverables and activities are subjected to a planning.

If a Safety plan is produced, it will be sent for acceptance before the contract award.

This document can be combined with a RAM Plan.

### 4.1.2 HAZARD ANALYSIS

The purpose of this analysis is to identify, characterize and classify the risks. Each Hazard related to the subsystem and the scope of the contract that is likely to occur during the life cycle of the subsystem will be assessed. In addition, the mitigation measures implemented to reach an acceptable risk level are identified and communicated according to the planning defined in the Safety plan.

### 4.1.3 FMEA / FMECA

The Failure Modes and Effects Analysis (FMEA) is a systematic, formal procedure for analysing a subsystem to identify potential failure modes, and their causes and effects on the functionality of the subsystem.

The FMECA (Failure Modes, Effects and Criticality Analysis) is an extension of the FMEA that includes a means of classifying failure modes by severity in order to give a priority to countermeasures.

A summary of all mitigation measures impacting hazards resulting from the FMECA analysis is communicated to Alstom.

Standard EN 60812 can be used as a reference.

This document can be combined to include both safety and reliability point of views.

### 4.1.4 FAULT TREE (SAFETY)

The aim of the fault tree is to demonstrate the proposed design achieves the specified safety requirements (quantitatively and qualitatively).

Fault trees are built starting from the so-called "top event" (typically a function failure or a feared event). This backward logic allows identifying which combinations of component failures could give rise to that top event and then minimal cuts which would not be obviously identified.

Assumptions and calculations rules shall be communicated with the supplied fault tree.

Standard EN 61025 can be used as a reference.

Other tools can be used (like Markov or petri net).

### 4.1.5 SAFETY MANAGEMENT FILE

The hazards identified, decisions made, solutions adopted and their implementation status are recorded in a management file or Hazard Log.

This file compiles evidences on the implementation of safety requirements regarding all identified hazards, thus supporting the demonstration of completeness of the safety assurance activities

All mitigation measures (or SRAC) under Alstom responsibility shall be extracted from this file (usually called hazard record).

## 4.2 ACTIVITIES BEFORE THE CONTRACT SIGNATURE

A preliminary description of the safety performances of the supplied product is required (main hazards and provisions). Alstom will analyse these performances and will share them with the Supplier to finalise a common approach.

The Supplier shall send the list of hazardous events considered for the design of his equipment / subsystem

The Supplier shall send the description of all known prevention measures that are (will be) used and documented to guarantee a high level of safety. For example:

- Application of recognised standards,
- Carry out tests (send the validation plan),
- Use subsystems / components certified by a reputable organisation,
- Use subsystems / components proven in practice,
- Respect qualitative requirements during the design (Redundancy – Fail Safe criterion, etc.),
- Respect quantitative requirements during the design (for example frequency at which a feared event occurs)
- Implementation of safety functions, or even evaluation of the capability of the subsystem / component to contribute performing a safety function (Safety Integrity Level "SIL" to be specified).

The supplier shall send the mitigations (SRAC) and main assumptions under Alstom responsibility if any.

A constructive response is expected (ie: with exchange of information) during the call for bids phase. In case of a compliance statement without relevant information provided, Alstom will consider that the Supplier has made a commitment to comply with any safety requirements defined during the system requirements allocation phase (neither extended times nor increased costs will be accepted).

The Supplier shall inform Alstom if it considers necessary to make a common safety study (for example this would be justified if integration of the component / subsystem is complex, if interfaces are potentially critical from a safety point of view).

## 4.3 ACTIVITIES DURING DEVELOPMENT PHASE

The Supplier shall communicate any new SRAC (all the SRAC are expected before contract award, refer to §4.2) as soon as possible to get general acceptance from Alstom. The final acceptance of the SRAC related to maintenance is communicated once accepted by the O&M.

The Supplier shall write a safety case that will contain all demonstrations to prove that the product is safe. At minimum it is required a statement that the system delivered is safe (then comply with the safety requirements defined by Alstom and Regulation if any). As example, the safety case shall include the following:

- A list of residual risks that repeats all requirements to be respected by other to achieve and maintain the high safety level expected. These SRAC may relate to:
  - Storage,
  - Integration,
  - Commissioning,
  - Operation,
  - Tests and inspections to be made,
  - Maintenance
  - Restrictions of use.

  The mitigation measures refer to exported safety requirements coming from safety analysis if any. The consolidated list provided by the Supplier can call a specific section of an existing document.
  When no SRAC are communicated, a statement shall be written to prevent any misunderstanding.
- Documents describing that all defined prevention measures have been correctly implemented:
  - Evidence of conformity with recognised standards,
  - Certificates for subsystems / components,
  - Justification file based on operating experience
  - Evidence of conformity with defined qualitative requirements,
  - Evidence that quantitative requirements are respected and therefore that:
    - Intervals between inspections (interval between two tests) used for the calculation are justified and are in agreement with the maintenance documentation written by the Supplier (for example a 24h test interval may be selected for a component that is tested automatically when the train is powered up).
    - The source of failure rates used is defined (operating experience, expert opinion, database).
    - Common cause failures (hardware and software) are evaluated.
    - Justification of compliance of the development to any Safety function relying on software shall be provided (typically compliance to EN50128).
    - Assumptions used for the study are listed.
    - Evidence that the instrumented safety functions achieve the defined safety integrity level, or even that the subsystem / component is capable of contributing to performing a safety function.
    - The list of identified dangerous failure modes,
    - etc.

The safety case is a way to formalize the Supplier commitment on Safety. The supplier is responsible to deliver a safe product compliant with regulation and all the safety tasks to be performed to operate and maintain it safe over its life expectancy.

The Supplier is responsible for the technical definition of his supply (configuration management and upgrade management). It shall define the configuration/version of the system under consideration to which the safety case applies and make sure that components and software critical for safety are traceable.

A preliminary safety case shall be sent before the start-up of series production. This report must be accepted by Alstom and it is compulsory for validation of the First Article Inspection (FAI).

Prior to the acceptance of series of equipment the safety case shall have been reviewed by Alstom. There shall be no blocking open point beside the ones related to activities planned after the acceptance such as test to be carried out on the train etc….Once the remaining validation activities are performed, the final version of the safety case will be issued not later than 1 month after and agreed by both Parties..

### 4.4 ACTIVITIES DURING THE OPERATION PHASE

The Supplier agrees that throughout the life of the component it shall:

- Analyse any failures critical for safety
- If necessary, recall and modify components / subsystems in operation
- Update predictive studies carried out and send the updated safety file to Alstom (as necessary).

## 5 TYPICAL SAFETY REQUIREMENTS

The Safety requirements are formalized and agreed prior contract award. On case by case basis (e.g. when a common safety study is needed), a specific action plan can be defined.

Safety demonstrations provided by the supplier will be reviewed and action closed when accepted by Alstom. The mitigations shall be clearly documented and performances maintained over the life of the product.

Interface with others equipment and associated safety requirements will be defined further and before contract award if any.

The specific functional safety requirements and targets are defined in the relevant TPS.

## 5.1 HVAC

| FSR | Functional Safety Requirements | Target |
|---|---|---|
| **FSR01** | Hazard: Asphyxia due to fire on board<br>Feared Event: Fire start or a smoke release from the HVAC<br>*Return of Experience stating the occurrence is improbable is recommended. | < 1 E-8 / h * |
| **FSR02** | Hazard: Projectile/pressure wave<br>Feared Event: HVAC explosion<br>*Return of Experience stating the occurrence is improbable is recommended. | < 1 E-8 / h * |
| **FSR03** | Hazard: Electrocution<br>Note: It shall cover all operations phases.<br>Feared Event: HVAC failures leading to electrocution (Voltage >=400 V)<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | < 1 E-9 / h * |
| **FSR04** | Hazard: Intoxication / Pollution<br>Feared Event: Failures leading to refrigerant leak outside the HVAC unit (apply when refrigerant is toxic)<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is improbable is recommended. | < 1 E-7 / h * |
| **FSR05** | Hazard: Collision/projectile<br>Feared Event: Failures leading to gauge fouling or fall/projection of HVAC parts<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | < 1 E-9 / h * |

## 5.2 PANTOGRAPH

| FSR | Functional Safety Requirements | Target |
|---|---|---|
| **FSR01** | Hazard: not able to cut-off or isolate HV supply<br>Feared Event: Not able to lower the pantograph given order is sent | < 1E-7/h |
| **FSR02** | Hazard: Catenary rupture<br>Feared Event: No adjustment in height of the pantograph leading to damage of the overhead line by arcing (dampers failure or others) | < 1E-7/h |
| **FSR03** | Hazard: Collision/projectile<br>Feared Event: Failures leading to gauge fouling or fall/projection of Pantograph parts<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | < 1E-9/h * |
| **FSR04** | Calculation note to demonstrate fixations are adequate and redundant. | N/A |
| **FSR05** | To demonstrate the effort needed to rise the pantograph is higher than the air pressure while running (both directions and taking into account worst consequences) | N/A |

## 5.3 DOORS

| FSR | Functional Safety Requirements | Target |
|---|---|---|
| **FSR01** | Hazard: People falling of train due to wrong side opening<br>Functional Requirement: To not allow door wrong side opening (up to SIL4 at Train level) | Supplier contribution tbd in TPS |
| **FSR02** | Hazard: People falling of train in operation or Collision due to fouling of the gauge<br>Functional Requirement: To maintain door/step closed when running (up to SIL4 at Train level) | Supplier contribution tbd in TPS |
| **FSR03** | Hazard: People falling of train in operation<br>Feared event: Loss of door closing effort allowing opening<br>*Qualitative demonstration accepted. | < 1E-9/h* |
| **FSR04** | Hazard: People falling of train in operation<br>Functional Requirement: To prevent the door opening in case of emergency handle actuation when train is in motion. (up to SIL2 at Train level) | Supplier contribution tbd in TPS |
| **FSR05** | Hazard: People falling of train at start-up or Collision due to fouling of the gauge<br>Functional Requirement: To not allow start-up when at least one door/step is not closed & locked (up to SIL4 at Train level) | Supplier contribution tbd in TPS |
| **FSR06** | Hazard: Departure of the train with something* or someone gripped by doors<br>Functional Requirement: To not start with a passenger trapped during closing/opening phase (up to SIL4 at Train level)<br>*: minimum size of the object specified in TPS | Supplier contribution tbd in TPS |
| **FSR07** | Hazard: Door locked closed (no emergency escape possible)<br>Functional Requirement: To open mechanically a door when door manual opening is required (up to SIL2 at Train level) | Supplier contribution tbd in TPS |
| **FSR08** | Hazard: Fall of passengers from vehicle on track by the door window<br>Qualitative requirement : Compliance to UIC 566 §2.1.2 (for UIC compliant rolling-stock) | N/A |
| **FSR09** | Hazard: Departure of the train with something or someone gripped by doors<br>Qualitative requirement : Compliance to EN14752 | N/A |
| **FSR10** | Hazard: People falling of train<br>Functional Requirement: Closed step wrongly detected as open and allows the door to open (up to SIL2 at Train level) | Supplier contribution tbd in TPS |

## 5.4 AUXILIARY BATTERY

The following requirements apply to the low-voltage batteries (ie to supply auxiliary equipment)

| FSR | Functional Safety Requirements | Target at train level |
|---|---|---|
| **FSR01** | Hazard: Projectile/pressure wave<br>Feared event: Projection of mechanical parts or fluid of the battery due to explosion of the battery (coming from internal failure causes)<br>*Return of Experience and recognized standard compliance (eg EN60529) stating the occurrence is improbable is recommended. | < 1E-9/h * |
| **FSR02** | Hazard: Asphyxia due to fire on board<br>Feared event: Fire start or smoke release from Battery | < 1E-8/h |
| **FSR03** | Hazard: Electrocution<br>Feared Event: Battery failure leading to electrocution<br>Note: It shall cover all operations phases. | < 1E-9/h |
| **FSR04** | Hazard: Projectile/pressure wave<br>Feared event: Presence of H2 gas cloud having a concentration between LEL (4%vol) and SEL (75%vol) or other explosive or toxic gas clouds. Calculations of necessary ventilation for battery boxes based on EN50272-2 or equivalent according to Boost charge current (Igas boost) and assuming an overvoltage of xxxV (worst ambient conditions to be taken)<br>Note: Exported safety constraints to limit potential ignition sources and regarding battery ventilation box outside Supplier scope shall be shared with Alstom if any. | < 1E-9/h |
| **FSR05** | Hazard: Collision/projectile<br>Feared event: Failures leading to gauge fouling or fall/projection of Battery parts<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | < 1E-9/h * |

## 5.5 COUPLER

Generic Functional Safety Requirements for automatic or semi-permanent couplers:

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01as** | Hazard: Collision/projectile<br>Feared event: failures leading to gauge fouling or fall/projection of coupler parts<br>* Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended | < 1E-9/h* |
| **FSR02as** | Calculation note to demonstrate fixations on carbody are adequate and redundant (when applicable) | No quantitative target |
| **FSR03as** | Mechanical tests compliant with the TPS requirements | No quantitative target |

Generic Functional Safety Requirements for automatic couplers:

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01a** | Hazard: Derailment/Collision<br>Feared event: Undue automatic coupler uncoupling<br>*Qualitative demonstration stating the occurrence is incredible is accepted. | < 1E-08/h* |
| **FSR02a** | Hazard: loss of brake performances potential for collision/derailment<br>Feared Event: Untimely complete or partial closure of the Brake Pipe and/or Main Pipe in a coupled status (when applicable)<br>*Qualitative demonstration stating the occurrence is incredible is accepted. | < 1E-9/h* |
| **FSR03a** | Hazard: Collision<br>Feared Event: Untimely uncoupling with a complete or partial closure of the Brake Pipe (when applicable)<br>*Qualitative demonstration stating the occurrence is improbable is accepted. | < 1E-7/h* |
| **FSR04a** | Hazard: loss of safety function relaying on train line<br>Feared Event : Untimely grounding of a low voltage train line (in coupled or uncoupled status) (When applicable)<br>*Qualitative demonstration stating the occurrence is improbable is accepted. | < 1E-7/h* |
| **FSR05a** | Hazard: loss of safety function relaying on train line<br>Feared Event : Untimely feeding of a low voltage train line with an energized low voltage line (in coupled or uncoupled status) (When applicable)<br>*Qualitative demonstration stating the occurrence is incredible is accepted. | < 1E-9/h* |
| **FSR06a** | Coupler compliant with EN60352 and IEC 61373 (to confirm robustness of electrical connections in line with FSR04 & FSR05)<br>Note: Discrepancy with IEC 61373 test requirements will be managed through the TPS if any will be added. | No quantitative target |

Generic Functional Safety Requirements for semi-permanent couplers:

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01s** | Hazard: Derailment/Collision<br>Feared event: Undue permanent or semi-permanent uncoupling<br>*Qualitative demonstration stating the occurrence is incredible is accepted. | < 1E-9/h* |

## 5.6 BRAKES

The defined failure modes consider the "full-scope" of brake system including brake control, air supply and bogie brake).

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01** | Hazard: Derailment/Collision<br>Feared event: Lost/Impaired Emergency brake at train level (leading to the non-respect of stopping distances or emergency brake minimum deceleration as specified in the TPS/LPA) | <1E-09/h |
| **FSR02** | Hazard: Derailment/Collision<br>Safety Requirement: Every single failure degrading the nominal emergency braking performance at train level (as specified in the TPS/LPA). All such failures shall be detected) | <1E-6/h |
| **FSR03** | Hazard: Derailment/fire<br>Feared event: Undue undetected Brake (all types of brake) application while running (up to 1E-9/h at Train level) | Supplier contribution tbd in TPS (in particular allocation between undue application vs detection) |
| **FSR04** | Hazard: Derailment/Collision<br>Functional requirement: WSP function failure jeopardizing the pneumatic braking performance at train level (leading to the non-respect of stopping distances or emergency brake minimum deceleration as specified in the TPS/LPA)<br>Note 1: A systematic WSP regulation failure properly mitigated after a defined temporisation by the watchdog will be considered in the emergency brake performance calculation.<br>Note 2: Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | <1E-09/h (note 2) |
| **FSR05** | Hazard: Collision due to drift of the train<br>Feared event: Loss of parking brake performance (as specified in the TPS) leading to drift of the train (up to 1E-9/h at Train level) | To be defined on a case by case basis according to the THR apportionment from train level |
| **FSR06** | Hazard: Collision due to drift of the train<br>Feared event: Undetected parking brake mechanical release per parking brake unit when human action is needed to reset/unlock the parking brake | <1E-6/h |
| **FSR07** | Hazard: Passenger injuries<br>Excessive jerk (as specified in the TPS) | To be demonstrated by validation test |
| **FSR08** | Hazard: Collision/projectile<br>Feared event: failures leading to gauge fouling or fall/projection of parts<br>* Qualitative demonstration relying on recognized standard compliance and stating the occurrence is incredible is recommended. | <1E-9/h* |
| **FSR09** | Hazard: People falling of train at start-up due to train drift<br>Functional requirement: To apply and maintain holding brake during passenger exchange (up to 1E-7/h at Train level) | Supplier contribution tbd in TPS |

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR10** | Hazard: People falling of train<br>Functional requirement: To provide the standstill/zero velocity information (up to 1E-7/h/SIL2) | Supplier contribution tbd in TPS |
| **FSR11** | Hazard: Derailment/Collision<br>Feared event: Undetected loss of pressure in the main pipe below the minimum threshold (as stated in the TPS) (Up to 1E-7/h at train level) | Supplier contribution tbd in TPS |

## 5.7 FIRE & SMOKE DETECTION (AND EXTINGUISHING) SYSTEM (FSD)

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01** | Hazard: Asphyxia due to fire on board<br>Functional Requirement: To detect fire in hazardous locations(1) and communicate the information through a LV output de-energized (up to SIL2(2)).<br>(1): Typically, MV/HV cubicles (like traction box, Main Transformer) or power pack. Items to be protected are specified in TPS.<br>(2): when required, software developed in accordance with SIL2 requirements of EN50128 or EN50657 and hardware in accordance with SIL2 requirement of EN50129 or equivalent. Compliance to EN50121 also required. | Supplier contribution tbd in TPS |
| **FSR02** | Hazard: Asphyxia due to fire on board<br>Functional Requirement: To release firefighting agent in defined location(s) when an order(1) is received (up to SIL2).<br>(1): type of order is specified in TPS (like LV input energized) | Supplier contribution tbd in TPS |
| **FSR02a(1)** | Hazard: Cancerogenic or toxic firefighting agent<br>Feared event: Untimely release(2) of firefighting agent when presence of person is foreseen (like during maintenance).<br>(1): Applicable when the safety requirement FSR02 applies and the firefighting agent is toxic (water mist being recommended).<br>(2): Release shall be prevented when the train is not in commercial service and appropriate ventilation requirement defined to ensure the access is safe after a release.<br>(3): Qualitative demonstration accepted. | ≤ 1E-9/h(3) |
| **FSR03** | Hazard: various<br>Qualitative requirement: Compliance with IEC61373, EN50155, environmental conditions defined for the project (e.g. tests in accordance with EN60068 performed) and EN45545(1)<br>(1): EN45545 requirements are specified in TPS if any | N/A |

## 5.8 MASTER CONTROLLER (MC)

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01** | Feared Events to be demonstrated for the complete system (driver's device, control lever, transfer mechanism and switch):<br>- Contact(1) NO blocked closed when it is released by the driver<br>- Contact(1) NO blocked opened when it is activated by the driver<br>- Contact(1) NC blocked open when it is released by the driver<br>- Contact(1) NC blocked closed when it is activated by the driver<br>Remarks :<br>- evaluation per contact, whatever the function performed<br>- Interlocking between contacts if any shall be documented<br>- Interlocking between sub-systems(2) if any shall be documented | < 1 E-7 / h |
| **FSR02** | Hazard: When removing the key to let a switch in an unwanted position<br>Feared Event: In the absence of cab Key, a contact(1) not in expected position<br>* Qualitative demonstration stating that the occurrence is improbable can be also accepted | < 1 E-7 / h* |
| **FSR03** | Hazard: Deadman not detected<br>Functional Requirement: To release the Deadman acknowledgement<br>Input: no more Driver acknowledgement<br>Treatment: when Deadman acknowledgement is released*, the output from E/PE** is set at 0 (de-energized)<br>* All the conditions used to acknowledge the Deadman shall be considered.<br>** Electronic/Programmable Electronic<br>*** software developed in accordance with SIL2 requirements of EN50128 or EN50657 and hardware in accordance with SIL2 requirement of EN50129 or equivalent. Compliance to EN50121 also required. | SIL2***<br><2E-7/h |
| **FSR04** | Hazard: Unwanted traction/brake order or effort requested greater than the one expected<br>Functional Requirement: To communicate the traction/brake effort based on the position of the Traction/Brake Handle.<br>Input: Position of the Traction/Brake Handle<br>Treatment: Given the position of the Traction/Brake Handle, the output from E/PE* is set as expected (Considering the redundancy if any).<br>* Electronic/Programmable Electronic<br>** software developed in accordance with Basic Integrity requirements of EN50128 or EN50657. | Basic Integrity**<br><2E-5/h |
| **FSR05** | Master Controller compliant with IEC61373, EN50155 and environmental conditions defined for the project (e.g. tests in accordance with EN60068 performed). | N/A |
| **FSR06** | Hazard: Emergency Brake order released<br>Qualitative requirement: The emergency braking position is notched and stable. | N/A |

**(1)** Applies for all contacts of Master Controller including Speed Direction, Key Switch, Mode Selector and Running Direction, if any.

**(2)** Traction/Brake Handle, Speed Direction, Key Switch, Mode Selector and Running Direction

## 5.9 TOILET

The Toilet supplier shall document that any credible hazard due to its scope of supply is well mitigated. At least the following hazards shall be analyzed:

| FSR | Functional Safety requirement | Target |
|---|---|---|
| **FSR01** | Hazard: Asphyxia due to fire on board<br>Feared Event: smoke release from the Toilet not detected**(1)**<br>* Qualitative demonstration stating the occurrence is improbable is recommended.<br>**(1)** On project basis detection relying on smoke detector installed and part of supplier scope of supply | ≤ 1 E-8 / h * |
| **FSR02** | Hazard: Electrocution<br>Note: It shall cover all operations phases (like maintenance).<br>Feared Event: Contact with part under voltage leading to electrocution<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is improbable is recommended. | < 1 E-7 / h * |
| **FSR03** | Hazard: Fall of parts<br>Feared Event: Failures leading to fall of Toilet parts<br>* Qualitative demonstration relying on safety cable stating the occurrence is improbable is recommended. | < 1 E-7 / h * |
| **FSR04** | Hazard: no emergency escape (considering also person with reduced mobility and door locked from outside)<br>Feared Event: Door failure leading to jeopardize emergency evacuation<br>*Qualitative demonstration relying on recognized standard compliance and stating the occurrence is improbable is recommended. | ≤ 1 E-7 / h* |
| **FSR05** | Hazard: Presence of sharp objects or pinch points<br>Feared Event: Passenger contact with a sharp object or pinch point* (e.g. when door closing)<br>* Pinch points as defined in EN12221-2 §5.3.1 to §5.3.3 or those specified in TPS apply | N/A |
| **FSR06(1)** | Hazard: Information not transmitted to the driver/ train crew<br>Feared Event: Passenger unable to call for help<br>* Qualitative demonstration stating the occurrence is improbable is accepted.<br>**(1):** Applicable when required by regulation (TSI PRM). | ≤ 1 E-7 / h * |
| **FSR07** | Hazard: various<br>Qualitative requirement: Compliance with IEC61373, EN50155, EN50153, environmental conditions defined for the project (e.g. tests in accordance with EN60068 performed) and EN45545**(1)**<br>(1): EN45545 requirements are specified in TPS if any | N/A |

| FSR | Functional Safety Requirements | Target |
|---|---|---|
| **FSR08** | Hazard: Drinking water contamination **(1) (2) (3)**<br>Feared Event: Drinking water contamination due to improper design or any kind of failure<br>* Qualitative demonstration relying on recognized standards compliance (like EN1717), qualified material used and manufacturing/storage prevent contamination and stating the occurrence is incredible is expected<br>**(1) :** Applies when drinkable water is specified. If not, the hazard shall be mitigated by appropriate safety warning.<br>**(2)** : Contamination from a passenger is excluded<br>**(3):** Exported constraints (SRAC) defined and shared (like cleaning requirement, maintenance constraints) | N/A* |

## 5.10 OTHER COMMODITIES

For other commodities not specifically detailed in the current revision of the present document the functional safety requirements will be defined in the relevant TPS.

# 6 SAFETY DELIVERABLES

The below list of safety deliverables is the by default list to be applied for each commodity. It can be adjusted based on project and product specificities. In case of specific requirements this shall be stated in the corresponding TPS.

| Ref | Subsystem Safety Typical deliverables list | BRAKES | DOORS | HVAC | COUPLER | BATTERY | PANTO | MC | FSD | TOILET |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Safety Plan | M | M | R | - | - | R | - | R | - |
| 2 | Hazard Analysis(4) | M | M | M | M | M | M | - | M when applicable (3) | M |
| 3 | Safety Management file (Hazard Log) (5) | - | - | - | - | - | - | - | - | - |
| 4 | FMEA/FMECA | M | M | HR | R | R | HR | M | M | HR |
| 5 | Safety Demonstrations (like FTA) | M | M | M when applicable (1) | M when applicable (1) | M when applicable (1) | M when applicable (1) | M | M when applicable (1) | M |
| 6 | SIL Demonstration | M when applicable (2) | M when applicable (2) | M when applicable (2) | - | M when applicable (2) | M when applicable (2) | M when applicable (2) | M when applicable (2) | M when applicable (2) |
| 7 | Safety Case (§4.3) | M | M | M | M | M | M | M | M | M |

M : Mandatory
HR : Highly Recommended
R : Recommended

**(1)** : When a demonstration of a feared event or a functional failure rate specified relies on the combination of failures (complementary with single failure analysis like FMEA/FMECA), the Supplier shall perform a safety demonstration other than FMEA/FMECA being a single failure analysis.

**(2)** : SIL Demonstration for Safety Functions relying on Electronic or Programmable Electronic shall be performed: random failure target is achieved and the required level of confidence on systematic failures (e.g. software development process and hardware part design) shall be justified.

**(3)** : Applies when the gas used for extinguishment is toxic

**(4)** : Hazard Analysis is under the supplier responsibility. When not requested, that means Alstom required only the summary in the Safety Case (including SRAC if any).

**(5)** : Safety Management file (Hazard Log) is under the supplier responsibility. That means Alstom requires only the status of the safety requirements coming from the supplier safety studies and those defined by Alstom in the Safety Case (including SRAC if any).

The below table provides the by default planning of expected delivery to Alstom of the safety deliverables.

| Ref | Safety Deliverables | Consultation | SGR | PGR | CGR | FAI | Warranty |
|---|---|---|---|---|---|---|---|
| 0 | Technical information as per §4.2 | P | | | | | |
| 1 | Safety Plan | P as per §4.2 | F | | | | |
| 2 | Hazard Analysis | P as per §4.2 | U | U | F | | |
| 3 | FMEA / FMECA | | | | P | F | |
| 4 | Safety Demonstration (like FTA) | | | | P | F | |
| 5 | SIL Demonstration | | | | P | F | |
| 6 | Safety Case (§4.3) | | | | P | F | As built* |

P = Preliminary; U = Update (as necessary); F = Final /As-built

*:The "as-built" is needed to reflect the safety related changes occurred during post FAI phase till end of warranty to have a safety case consistent with the as-built product. If no changes affecting the safety then Alstom just needs an updated document stating that the conclusions of the FAI safety case still applies to the as-built version of the product.