Collaborative Large-scale Integrating Project

Open Platform for EvolutioNary Certification Of Safety-critical Systems

List of proposed requirements for Railway domain
Annex D1.1.c to deliverable D1.1

Work Package:	WP1: Use case Specification and Benchmark
Dissemination level:	PU = Public
Status:	FINAL
Date:	28 March 2012
Responsible partner:	F. Tagliabò (CRF)
Contact information:	fulvio.tagliabo@crf.it

Contributors

Names	Organisation
Laurent Pitot de la Beaujardière, Fabien Belmonte	ALSTOM Transport

Document History

Version	Date	Remarks
V0.1	2012-03-15	First emission
V0.2	2012-03-20	Ready for PB Approval
V1.0	2012-03-28	Approved by PB

TABLE OF CONTENTS

1 SAFETY POLICY

The proposed railway requirements which constitute “Safety Policy” according to the reference standard are detailed in the following:

<ALS> 0001: <Safety Culture>	
Alias	Independence of checks and balances
Status	Proposed
App. Domain	Railway
Type	Safety Policy
Priority	High
Description	Appropriate degree of independence in the safety and engineering processes (safety, quality, verification, validation and management)
Derived from	EN50126 Part 6

<ALS> 0002: <Safety Culture>	
Alias	Evidence of Safety performance monitoring
Status	Proposed
App. Domain	Railway
Type	Safety Policy
Priority	High
Description	The organization shall institute, execute and maintain a field monitoring process with respect to the item's functional safety (including the reporting of incidents, the measures for correction, the recall and the corresponding decision-making processes)
Derived from	EN50126 Part 6 – Phase 12

<ALS> 0003: <Safety Competences>	
Alias	Evidence of competence
Status	Proposed
App. Domain	Railway
Type	Safety Policy
Priority	High
Description	To evaluate internally that the organization involves persons with competences and categories corresponding to their responsibility and the same for its suppliers
Derived from	EN50126 Part 6

<ALS> 0004: <Safety Competences>	
Alias	Competence assessment
Status	Proposed
App. Domain	Railway
Type	Safety Policy
Priority	High
Description	The competence of personnel undertaking tasks within the system requirement phase shall be assessed.
Derived from	EN 50126-1 Phase 4

<ALS> 0005: <Quality standard>	
Alias	Evidence of quality management
Status	Proposed
App. Domain	Railway
Type	Safety Policy
Priority	High
Description	To evaluate internally that the organization is compliant with quality reference standards
Derived from	EN50129 Clause 5

2 SAFETY PROCESSES

The proposed railway requirements which constitute “Safety Processes” are detailed in the following:

<ALS> 0006: <Completeness and Compliance>	
Alias	Review of the safety plan and safety case
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	The internal safety assessor shall perform review of the safety plan and safety case
Derived from	Internal Safety Policy

<ALS> 0007: <Completeness and Compliance>	
Alias	Review of the hazard analysis and risk assessment
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	The head of the safety department shall perform review of the hazard analysis and risk assessment
Derived from	Internal Safety Policy

<ALS> 0008: <Completeness and Compliance>	
Alias	Review of the validation plan
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	The Project Safety Assurance Manager shall approve the validation plan
Derived from	Internal Safety Policy

<ALS> 0009: <Completeness and Compliance>	
Alias	Acquire scope, context and purpose of the system
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	to acquire, in the context of safety performance, an understanding of: a) the scope, context and purpose of the system. b) the environment of the system, including: • physical issues; • potential system interface issues; • social issues; • political issues; • legislative issues; • economical issues.

	c) the general safety implications of the system.
Derived from	EN50126 Phase 1

<ALS> 0010: <Completeness and Compliance>	
Alias	Review financial and feasibility issues
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Review financial and feasibility issues: a) the safety implications of any financial analysis of the system. b) the safety implications of any system feasibility studies.
Derived from	EN50126 Phase 1

<ALS> 0011: <Completeness and Compliance>	
Alias	identify sources of hazards
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	to identify sources of hazards which could affect the safety performance of the system, including: • interaction with other systems; • interaction with humans.
Derived from	EN50126 Phase 1

<ALS> 0012: <Completeness & Compliance>	
Alias	Define Safety Policy and Targets
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Define Safety Policy and Targets including provision of information about: a) previous safety requirements and past safety performance of similar and/or related systems. b) identified sources of hazards to safety performance. c) current Railway Authority Safety Policy and Targets. d) safety legislation.
Derived from	EN50126 Phase 1

<ALS> 0013: <Completeness and Compliance>	
Alias	define management scope
Status	Proposed
App. Domain	Railway

Type	Safety Processes
Priority	High
Description	to define the scope of the management requirements for subsequent system lifecycle safety tasks.
Derived from	EN50126 Phase 1

<ALS> 0014: <Completeness and Compliance>	
Alias	Define system boundary and safety scope
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Define system boundary and safety scope: a) the system mission profile, including: – performance requirements; – Safety targets; – long term operating strategy and conditions; – long term maintenance strategy and conditions; – system life considerations, including lifecycle costing issues; – logistic considerations. b) the system boundary, including: – interfaces with physical environment; – interfaces with other technological systems; – interfaces with humans; – interfaces with other Railway Authorities. c) the scope of application conditions influencing the system, including: – constraints imposed by existing infrastructure; – system operating conditions; – system maintenance conditions; – logistic support considerations; – review of past experience data for similar systems. d) the scope of the system hazard analysis, including the identification of: – hazards inherent within the process to be controlled; – environmental hazards; – security hazards; – the influence of external events; – the boundaries of the system to be analysed; – the influence on safety of existing infrastructure constraints.
Derived from	EN50126 Phase 2

<ALS> 0015: <Completeness and Compliance>	
Alias	preliminary hazard identification
Status	Proposed
App. Domain	Railway
Type	Safety Processes

Priority	High
Description	Perform preliminary hazard identification to: * identify sub-systems associated with identified hazards; * identify types of accident initiating events that need to be considered, including component failure, procedural faults, human error and dependent failure mechanisms; * define initial risk tolerability criteria.
Derived from	EN50126 Phase 2

<ALS> 0016: <Completeness and Compliance>	
Alias	establish the general safety policy
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Establish the general safety policy for the system, including requirements of safety concept and the Railway Authority's' policy for resolving any conflicts arising between "availability" and "safety".
Derived from	EN50126 Phase 2

<ALS> 0017: <Completeness and Compliance>	
Alias	Perform risk analysis
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Perform risk analysis including the following steps : a) Systematically identify and prioritise all reasonably foreseeable hazards associated with the system in its application environment. b) identify the sequence of events leading to hazards. c) evaluate the frequency of occurrence of each hazard. d) evaluate the likely severity of the consequences of each hazard. e) evaluate the risk to the system for each hazard.
Derived from	EN50126 Phase 3

<ALS> 0018: <Completeness and Compliance>	
Alias	classify the acceptability of the risk
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and

	lifecycle cost requirements of the system.
Derived from	EN50126 Phase 3

<ALS> 0019: <Completeness and Compliance>	
Alias	establish a Hazard Log
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Establish a Hazard Log as the basis for on-going risk management. The Hazard Log shall be updated, whenever a change to any identified hazard occurs or a new hazard is identified, throughout the lifecycle. Hazard Log shall include details of: a) the aim and purpose of the Hazard Log. b) each hazardous event and contributing components. c) likely consequences and frequencies of the sequence of events associated with each hazard. d) the risk of each hazard. e) risk tolerability criteria for the application. f) the measures taken to reduce risks to a tolerable level, or remove, the risk for each hazardous event. g) a process to review risk tolerability. h) a process to review the effectiveness of risk reduction measures. i) a process for on-going risk and accident reporting. j) a process for management of the Hazard Log. k) the limits of any analysis carried out. l) any assumptions made during the analysis. m) any confidence limits applying to data used within the analysis. n) the methods, tool and techniques used. o) the personnel, and their competencies, involved in the process.
Derived from	EN50126 Phase 3

<ALS> 0020: <Completeness and Compliance>	
Alias	Specify the overall safety requirements for the total system
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The Safety Requirements, for the system under consideration, shall include: − definition of the system and boundaries; − mission profile; − functional requirements and supporting performance requirements, including

	safety functional requirements and safety integrity requirements for each safety function; − logistic support requirements; − interfaces; − application environment; − tolerable risk levels for identified hazards; − external measures necessary to achieve the requirements; − system support requirements; − details of the limits of the analysis; − details of any assumptions made.
Derived from	EN 50126-1 Phase 4

<ALS> 0021: <Completeness and Compliance>	
Alias	Requirements for achieving compliance with safety requirement
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The specification of the overall requirements for achieving compliance with safety requirements for the system shall include: - acceptance criteria for the overall safety requirements; - demonstration and acceptance process for the overall safety requirements facilitated by the system safety validation plan, which should include: o a description of the system; o the safety validation principles to be applied to the system; o the safety tests and analysis to be carried out for the validation including details of the required environment, tools, facilities etc.; o the validation management structure including requirements for personnel independence; o details of the validation program (sequence and schedule); o procedures for dealing with noncompliance.
Derived from	EN 50126-1 Phase 4

<ALS> 0022: <Completeness and Compliance>	
Alias	Migration / use of other standards
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Migration from other standards or use of compliance to other standards requires that both systematic and random failures are controlled in a way that is compliant to EN 50129 and EN 50128.
Derived from	EN50129

<ALS> 0023: <Completeness and Compliance>	
Alias	Hazard Log
Status	Proposed
App. Domain	Railway

Type	Safety Processes
Priority	High
Description	A Hazard Log shall be used to record the identified causes of failing to meet safety requirements (hazards) and the evidence of management in the design, build, operation and maintenance of the technical system. The Hazard Log should be supported by both a top down hazard identification process and a bottom up cause identification process such as FMEA.
Derived from	EN50129 Safety Case Part 3

<ALS> 0024: <Completeness and Compliance>	
Alias	Specification and Design of Safety Requirements
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Evidence will be given regarding the coverage in Specification and Design of System / Sub-system / Equipment Safety Requirements as identified in the safety analysis (Risk Analysis, Hazard Analysis).
Derived from	EN50129 Safety Case Part 3

<ALS> 0025: <Audit>	
Alias	Safety Reviews and/or Safety Audits
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Safety Reviews and/or Safety Audits shall be performed to provide a systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements.
Derived from	EN50129 Safety Case Part 3

<ALS> 0026: <Completeness and Compliance>	
Alias	Review of impact analysis of modifications
Status	Proposed
App. Domain	Railway
Type	Safety Processes
Priority	High
Description	Evolutions/modifications shall be managed according to dedicated quality procedures, including review by the safety manager in order to identify which lifecycle phases and products are impacted.
Derived from	EN50129 Safety Case Part 3

<ALS> 0027: <Completeness and Compliance>	
Alias	Requirements verification
Status	Proposed
App. Domain	Railway
Type	Safety Process

Priority	High
Description	System requirements shall be verified against the deliverables produced within concept phase and system definition phase, including lifecycle costings. Safety requirements shall be verified against any safety targets and safety policies of the Railway Authority.
Derived from	EN 50126-1 Phase 4

<ALS> 0028: <Completeness and Compliance>	
Alias	Adequacy and completeness of the Acceptance Plan and the Validation Plan
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The Adequacy and the completeness of the Acceptance Plan and the Validation Plan shall be assessed.
Derived from	EN 50126-1 Phase 4

<ALS> 0029: <Completeness and Compliance>	
Alias	Methods, tools and techniques assessment
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The methods, tools and techniques used within the system requirement phase shall be assessed.
Derived from	EN 50126-1 Phase 4

<ALS> 0030: <Completeness and Compliance>	
Alias	Requirement allocation
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	a) Allocate functional requirements to designated sub-systems, components and external facilities. b) Allocate safety requirements to designated sub-systems, components and external risk reduction facilities.
Derived from	EN 50126-1 Phase 5

<ALS> 0031: <Completeness and Compliance>	
Alias	Requirements for compliance with subsystem
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The requirements for compliance with subsystem, component and external facilities requirements shall be specified, including:

	– acceptance criteria for sub-system, component and external facilities requirements; – demonstration and acceptance processes and procedures for sub-system, component and external facilities requirements.
Derived from	EN 50126-1 Phase 5

<ALS> 0032: <Completeness and Compliance>	
Alias	Requirement Apportionment verification
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The following verification shall be realized: – Verification of system, sub-system, component and external facility requirements against the deliverables produced in phase 4, and including a review of the requirements against the lifecycle cost for the system; – The architecture for the total combination of designated sub-systems, components and external facilities shall be verified to ensure it complies with the Safety requirements for the total system; – The safety requirements for sub-system, component and external facilities shall be verified to ensure that they are traceable to the RAMS requirements for the system; – The safety requirements for sub-system, component and external facilities shall be verified to ensure completeness and consistency between functions; – The revised Safety plan and Validation plan shall be verified to ensure its continued applicability; – Assessment of the adequacy of the methods, tools and techniques used within the phase – Assessment of the competence of all personnel undertaking tasks within the apportionment phase.
Derived from	EN 50126-1 Phase 5

<ALS> 0033: <Completeness and Compliance>	
Alias	Safety requirement satisfaction
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The design and the realization of the sub-systems and components shall meet the safety requirements
Derived from	EN 50126-1 Phase 6

<ALS> 0034: <Completeness and Compliance>	
Alias	Manufacturing process
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High

Description	The design and implementation phase shall define, verify and establish a manufacturing process capable of producing Safety-validated sub-systems and components, giving consideration to the use of: – Environmental stress screening; – Inspection and testing for Safety-related failure modes; – Details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle.
Derived from	EN 50126-1 Phase 6

<ALS> 0035: <Completeness and Compliance>	
Alias	Record safety validation tasks
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	A record of all safety validation tasks undertaken within the design and implementation phase shall be maintained.
Derived from	EN 50126-1 Phase 6

<ALS> 0036: <Completeness and Compliance>	
Alias	Safety verification within design and implementation
Status	Proposed
App. Domain	Railway
Type	Safety Process
Priority	High
Description	The following verification tasks shall be undertaken within the design and implementation phase: a) assessment of the adequacy of the information, and where appropriate, data and other statistics, used as input to tasks within this phase. b) verification, by analysis and test, that sub-system and component design complies with the RAMS requirements. c) verification, by analysis and test, that sub-systems and components realization complies with designs. d) validation of sub-system and component realization to ensure that the realization complies with RAMS acceptance criteria for sub-system and components, including lifecycle requirements. e) verification, by analysis and test, that the manufacturing arrangements produce Safety-validated sub-systems and components. f) verification that all future lifecycle activity plans are consistent with Safety requirements for the system, including lifecycle cost requirements. g) assessment of the adequacy and completeness of the generic safety case and where appropriate, the application safety case. h) assessment of the adequacy of the methods, tools and techniques used within the phase. i) assessment of the competence of all personnel undertaking tasks within the phase. j) ensure the continued applicability of the Safety validation plan.
Derived from	EN 50126-1 Phase 6

3 SAFETY PLANNING

The proposed railway requirements which constitute "Safety Planning" according to the reference standard are detailed in the following:

<ALS> 0037: <Safety plan>	
Alias	Project safety plan
Status	Proposed
App. Domain	Railway
Type	Safety Planning
Priority	High
Description	The safety activities for the system/sub-system/equipment development shall be planned including determination of appropriate methods and measures during design and validation
Derived from	EN50126 part 5

<ALS> 0038: <Safety Plan>	
Alias	establish the Safety Plan
Status	Proposed
App. Domain	Railway
Type	Safety Planning
Priority	High
Description	Establish the Safety Plan for the system. The Safety Plan shall be agreed by the Railway Authority and the railway support industry for the system under consideration and shall be implemented, reviewed and maintained throughout the lifecycle of the system. The Safety Plan should include: a) the policy and strategy for achieving safety. b) the scope of the plan. c) a description of the system. d) details of roles, responsibilities, competencies and relationships of bodies undertaking tasks within the lifecycle. e) description of the system lifecycle and safety tasks to be undertaken within the lifecycle along with any dependencies. f) the safety analysis, engineering and assessment processes to be applied during the lifecycle. g) details of all safety related deliverables from the lifecycle. h) a process to prepare system Safety Cases. i) a process for the safety approval of the system. j) a process for safety approval of system modifications. k) a process for analysing operation and maintenance performance to ensure realised safety is compliant with requirements. l) a process for the maintenance of safety-related documentation, including a Hazard Log.

	m) interfaces with other related programmes and plans. n) constraints and assumptions made in the plan. o) subcontractor management arrangements. p) requirements for periodic safety audit, safety assessment and safety review, throughout the lifecycle and appropriate to the safety relevance of the system under consideration, including any personnel independence requirements.
Derived from	EN50126 Phase 2

<ALS> 0039: <Safety Plan>	
Alias	Safety requirement consistency with safety plan
Status	Proposed
App. Domain	Railway
Type	Safety Planning
Priority	High
Description	The Safety Plan shall be amended to ensure that all future planned tasks are consistent with the system's emergent safety requirements.
Derived from	EN 50126-1 Phase 4

<ALS> 0040: <Safety Plan>	
Alias	Safety plan and validation plan review and update
Status	Proposed
App. Domain	Railway
Type	Safety Planning
Priority	High
Description	The Safety Plan and the Validation Plan shall be reviewed and updated to ensure that planned tasks are consistent with the requirements of the system following apportionment. Key areas of concern include requirements for personnel independence and the control of system interfaces where safety functionality may be compromised.
Derived from	EN 50126-1 Phase 5

<ALS> 0041: <Safety Plan>	
Alias	Future life cycle tasks planning
Status	Proposed
App. Domain	Railway
Type	Safety Planning
Priority	High
Description	Plans for future lifecycle tasks shall be established, including: – Installation; – Commissioning; – Operation and Maintenance, including definition of operation and maintenance procedures; – Data acquisition and assessment during operation.
Derived from	EN 50126-1 Phase 6

4 SAFETY PRODUCT

The proposed railway requirements which constitute “safety product” according to the reference standard are detailed in the following:

<ALS> 0042: <Boundary definition>	
Alias	Item definition
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	Complete definition of the item under development and its interfaces, including a system model allocating items to their respective safety scopes as generic product, generic application, or specific application.
Derived from	EN50126 Part 6 Phase 2

<ALS> 0043: <Boundary definition>	
Alias	Impact analysis
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	An analysis that has the aim to identify and describe the intended modification applied to the item or its environment and to assess the impact of these modifications
Derived from	EN50126 Part 6 Phase 13

<ALS> 0044: <Safety Case>	
Alias	Prepare a safety case
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	A Generic Safety Case for the system shall be prepared, justifying that the system, as designed and independent of application, meets safety requirements. The Safety Case requires approval by the Railway Authority, and should include: – an overview of the system; – a summary or reference to the safety requirements, including a consideration of the SIL justifications for safety functions; – a summary of the quality and safety management controls adopted within the lifecycle; – a summary of safety assessment and safety audit tasks; – a summary of safety analysis tasks; – an overview of the safety engineering techniques employed within the system – verification of the manufacturing process; – adequacy of compliance with safety requirements, including any SIL

	requirements of the system; – a summary of any limitations and constraints applying to the system; – any special exemption (or specificity) imposed and justified by the contract, to the – usual requirements of this Standard.
Derived from	EN 50126-1 Phase 6

<ALS> 0045: <Safety Case>	
Alias	Prepare an application safety case
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	An Application Safety Case shall be prepared, if appropriate at this stage, for the system. The Application Safety Case builds on the Generic Safety Case, justifying that the design of the system and its physical realization, including installation and test phases, for a specific class of application, meet safety requirements. The Application Safety Case requires approval by the Railway Authority, and should include: – all additional information necessary to justify system safety for the class of application under consideration; – any limitations or constraints relevant to the application of the system.
Derived from	EN 50126-1 Phase 6

<ALS> 0046: <Safety Case>	
Alias	Quality Management Report
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall include a quality management report including • Presentation of Quality System, Quality Plan and Quality Organisation • Evidence of Quality Management • Quality audits and inspections • Summary and Conclusions on the Quality Management
Derived from	EN50129 Safety Case Part 2

<ALS> 0047: <Safety Case>	
Alias	Safety Management Report
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Management Report is used to demonstrate that: • the project has been defined, developed and produced in accordance with a safety management process which is consistent with the management process for the Dependability (RAMS) indicated by the EN 50126; • the organisational structure adopted complies with the EN 50129, 5.3.3.
Derived from	EN50129 Safety Case Part 3

<ALS> 0048: <Safety Case>	
Alias	Safety Management Report
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall justify that the installed safety management and the range of the accompanying documentation of the regarded system/subsystem is appropriate for the Safety Integrity Level. A complete description listing the applicable phases of the lifecycle phases as defined in EN 50126 and related safety activities and safety documents shall be provided.
Derived from	EN50129 Safety Case Part 3

<ALS> 0049: <Safety Case>	
Alias	Safety Management Report
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	This section shall report the details of the Safety Organisation established for the project according to EN 50129, 5.3.3. In this section of the Safety Management Report it shall be reported that the safety management process is accomplished under control of a suitable organization, including reference to the degree of independence among actors.
Derived from	EN50129 Safety Case Part 3

<ALS> 0050: <Verification and Validation>	
Alias	Safety verification and validation
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall present evidence verifying that each phase of the life-cycle satisfies the specific safety requirements identified in the previous phase, and for validating the completed system/subsystem/equipment against its original Safety Requirements Specification.
Derived from	EN50129 Safety Case Part 3

<ALS> 0051: <Safety Case>	
Alias	Technical Safety Report
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall present a summary of the safety principles, the extent of safety measures and the list of reference standards relevant to the considered system,

	subsystem, equipment, including : • evidence to demonstrate the correct operation under fault-free normal conditions and to describe how safety requirements are fulfilled; • evidence demonstrating how safety requirements continue to be met in the event of random hardware faults
Derived from	EN50129 Safety Case Part 4

<ALS> 0052: <Safety Case>	
Alias	Operation with external influences
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall present evidence concerning the ability of the system/sub-system/equipment to operate correctly and safely when subjected to specified external influences. "Correct operation" includes fulfilment of both operational and safety requirements.
Derived from	EN50129 Safety Case Part 4

<ALS> 0053: <Safety measures review>	
Alias	Safety Related Application conditions
Status	Proposed
App. Domain	Railway
Type	Safety Product
Priority	High
Description	The Safety Case shall specify (or reference) the rules, conditions and constraints which shall be observed in the application of the system/sub-system/equipment. This shall include the application conditions contained in the Safety Case of any related sub-system or equipment.
Derived from	EN50129 Safety Case Part 4