PD CLC/TR 50506-2:2009

Railway applications — Communication, signalling and processing systems — Application guide for EN 50129

Part 2: Safety assurance

National foreword

This Published Document is the UK implementation of CLC/TR 50506-2:2009.

The UK participation in its preparation was entrusted by Technical Committee GEL/9, Railway Electrotechnical Applications, to Subcommittee GEL/9/1, Railway Electrotechnical Applications - Signalling and communications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 58285 1

ICS 93.100

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 January 2010

Amendments issued since publication

Amd. No.	Date	Text affected

PD CLC/TR 50506-2:2009

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CLC/TR 50506-2

December 2009

ICS 93.100

English version

Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129 - Part 2: Safety assurance

This Technical Report was approved by CENELEC on 2009-07-17.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: Avenue Marnix 17, B - 1000 Brussels

Foreword

This Technical Report was prepared by SC 9XA, Communication, signalling and processing systems, of Technical Committee CENELEC TC 9X, Electrical and electronic applications for railways.

The text of the draft was submitted to vote in accordance with the Internal Regulations, Part 2, Subclause 11.4.3.3 (simple majority) and was approved by CENELEC as CLC/TR 50506-2 on 2009-07-17.

____

Contents

Figures

Tables

Introduction

EN 50129 was developed in CENELEC and is now regularly called up in specifications. In essence, it lists factors that influence RAMS (see EN 50126-1) and adopts a broad risk-management approach to safety. EN 50129 is the basic standard for safety related electronic systems for signalling.

Use of EN 50129 has enhanced the general understanding of the issues, but also showed, that items like Safe Design, Safety Documents and Reports, Safety Assessment and Approval, and Cross-Acceptance need further explanation and clarification. Therefore CENELEC decided to address those items in this Application Guideline. The Cross Acceptance is included in CLC/TR 50506-1.

1 Scope

This document is a Technical Report about the basic standard. It is applicable to the same systems and addresses the same audience as the standard itself. It enhances information on specific items on the application of EN 50129. The following items are covered, within the scope of this Application Guideline of EN 50129, as follows:

- Clause 4 deals with identification and mitigation of failures in the concept, specification and design phases. It is mainly dedicated to designers and verifiers and product safety engineers;
- Clause 5 deals with the preparation of a safety case, enhancing points providing the required evidence for safety assessment and approval. It is mainly dedicated to verifiers, validators, safety managers, quality managers and safety engineers;
- Clause 6 deals with the activities an Independent Safety Assessor has to carry out. It is mainly dedicated to safety assessors, safety authorities, safety managers and safety approvals.

In drafting this guidance, it is assumed that the reader is familiar with the basic structure of the standard.

This document does not claim to be exhaustive. It is not a complete compilation of best practices, but only the translation of the knowledge of all the experts of the Working Group in charge of composition of this Application Guideline.

2 References

This Application Guideline uses as basis for specific topics the following reference standards, already mentioned in the main EN 50129.

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

CLC/TR 50506-1, *Railway applications – Communication, signalling and processing systems – Application Guide for EN 50129 – Part 1: Cross-acceptance*

EN 45004 [1], *General criteria for the operation of various types of bodies performing inspection*

EN 50121 series, *Railway applications – Electromagnetic compatibility*

EN 50121-4, *Railway applications – Electromagnetic compatibility – Part 4: Emission and immunity of the signalling and telecommunications apparatus*

EN 50124-1, *Railway applications – Insulation coordination – Part 1: Basic requirements – Clearances and creepage distances for all electrical and electronic equipment*

EN 50125-1, *Railway applications – Environmental conditions for equipment – Part 1: Equipment on board rolling stock*

EN 50125-2, *Railway applications – Environmental conditions for equipment – Part 2: Fixed electrical installations*

EN 50125-3, *Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications*

[1] Superseded by EN ISO/IEC 17020:2004, *General criteria for the operation of various types of bodies performing inspection* (ISO/IEC 17020:1998).

EN 50126-1:1999 + corr. May 2006, *Railway Applications – The specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process*

EN 50128, *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*

EN 50129:2003, *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

EN 50155, *Railway applications – Electronic equipment used on rolling stock*

EN 50159-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety related communication in closed transmission systems*

EN 50159-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety related communication in open transmission systems*

EN 61508 series, *Functional safety of electrical/electronic/programmable electronic safety-related systems* (IEC 61508 series)

EN ISO 9001:2000 [2], *Quality Management Systems – Requirements* (ISO 9001:2000)

ESA PSS 01-403, *Hazard Analysis and Safety Risk Assessment*

ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

The following standard is mentioned as complementary source of information:

EN ISO/IEC 17020 (former EN 45004), *General criteria for the operation of various types of bodies performing inspection* (ISO/IEC 17020)

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50126-1:1999, EN 50128:2001, EN 50129:2003 and the following apply.

3.1.1
generic application
system with specific functions that are related to “a category of applications” associated with a general environmental and operational context, which is developed on the basis of criteria of standardization and parameterization of its elements, so as to render it serviceable for various tangible applications. By combining generic products or combining these with other generic applications, it is possible to obtain a new generic application

3.1.2
generic product
component or product capable of performing certain functions, with specific performance level, in the environmental and operational conditions stated in the reference specifications. It can be combined with other products and Generic Applications to form other generic applications

[2] Superseded by EN ISO 9001:2008, *Quality management systems – Requirements* (ISO 9001:2008).

3.1.3
specific application
specific application addresses a specific installation for a dedicated project with specific implementation, as for instance data configuration

3.1.4
risk analysis
systematic use of all available information to identify hazards and to estimate the risk

[ISO/IEC 73:2002, Clause A.10]

3.1.5
safety analysis
subset of risk analysis solely focused on hazards which have a potential for causing accident which may cause harm to people

3.2 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

AC	Alternating Current
ASIC	Application Specific Integrated Circuit
ATC	Automatic Train Control
ATP	Automatic Train Protection
C	Customer
CCF	Common-cause failure
COTS	Commercial-Off-The-Shelf
CV	Curriculum Vitae
DC	Direct Current
DMA	Direct Memory Access
EM	Electro Magnetic
EMI	Electro Magnetic Interference
ESA PSS	Spacecraft and Associated Equipment – Procedures, Standards and Specifications
ESD	Electro Static Discharge
EU	European Union
EPLD	Erasable and Programmable Logic Device
ETA	Event Tree Analysis
FMEA	Failure Mode Effects Analysis (see also below)
FMECA	Failure Mode Effects and Criticality Analysis
FPGA	Field Programmable Gate Array

FTA	Fault Tree Analysis
FTI	Formal Technical Inspection
HAZOP	Hazard and Operability Study
HW	Hardware
I/O	Input / Output
ISA	Independent Safety Assessor
LRU	Line Replaceable Unit
PAL	Programmable Array Logic
PCB	Printed Circuit Board
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
QAP	Quality Assurance Plan
QMS	Quality Management System
R	Recommended
RAM	Reliability Availability Maintainability
RAMS	Reliability Availability Maintainability and Safety
RBD	Reliability Block Diagram
RS	Rolling Stock
S	Supplier
SART	Structured Analysis for Real Time
SC	Safety Case
SADT	Structured Analysis and Design Techniques
SRAC	Safety Related Application Condition
SHA	System Hazard Analysis
SIL	Safety Integrity Level
SMP	Safety Management Process
SRIL	Safety Related Item List
SRS	System Requirements Specification
SSRS	Subsystem Requirements Specification
SW	Software

TSR	Technical Safety Report
VHDL	VHSIC (Very High Speed Integrated Circuit) Hardware Description Language
VLSI	Very Large Scale Integration
V&V	Verification and Validation
µP	Micro Processor

4 Safety design for signalling subsystems

The design of signalling systems should follow the requirements specified in EN 50129:2003, 5.3 and, in particular, the safety design depends on the safety life-cycle which is consistent with the system life-cycle defined in EN 50126-1 (see EN 50129:2003, Figure 4).

This clause gives more explanations on two specific items of the safety design dealing with “Safety Requirements Specifications” covered by Safety Principles and “Hardware Design” covered by Components Development Guidance:

- safety principles, to be justified in early design phases of Products, Systems and Processes in particularly for platforms. These principles have also to be justified in the "Effects of Faults" subsection of every related Safety Case;
- components development guidance, mainly for programmable devices.

4.1 Safety principles

This subclause is in line with EN 50129:2003, 5.4 and gives more details on how to fulfil all the requirements specified in this subclause of the standard to provide technical evidences for the safety of the design and in particular for the identification and the mitigation of systematic and random failures.

All assumptions detailed here after should be applied to products.

4.1.1 Classes of faults, errors and failures

This subclause is in line with EN 50129:2003, 5.4 and in particular with Section 3 “Effects of faults” in which there is no clear definition of a Fault and no clear explanation of the relationship between faults, errors and failures. The following definitions are issued from CENELEC.

Fault: an abnormal condition that could lead to an error in a system. A fault can be random or systematic.

Error: a deviation from the intended design which could result in unintended system behaviour or failure (EN 50129).

Failure: a deviation from the specified performance of a system. A failure is the consequence of a fault or error in the system.

Hazard: a condition that could lead to an accident.

Remark: Hazards are not events (ESA PSS 01-403).

Let’s consider a functional unit (FU) viewed as a hierarchical composition of multiple levels, each of which can in turn be called a functional unit (Figure 1).

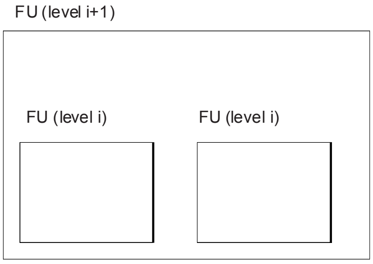


Figure 1 – Example for hierarchical composition of Functional units

The creation and manifestation mechanisms of faults, errors, and failures are illustrated by Figure 2, and summarized as follows.

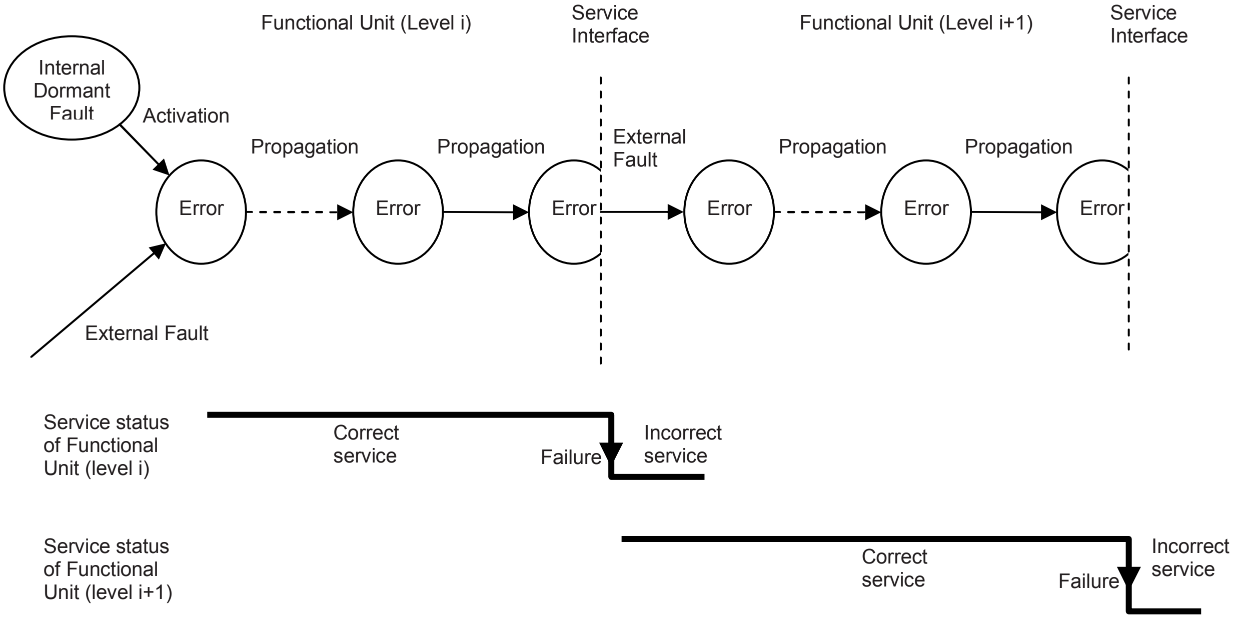


Figure 2 – Example for creation and manifestation mechanisms of faults, errors, and failures

1. A fault is active when it produces an **error**, otherwise it is **dormant**. An active fault is either a) an internal fault that was previously dormant and that has been activated by the computation process or environmental conditions, or b) an external fault. **Fault activation** is the application of an input (the activation pattern) to a FU that causes a dormant fault to become active. Most internal faults cycle between their dormant and active states.

2. Error propagation within a given FU (i.e., internal propagation) is caused by the computation process: an error is successively transformed into other errors. Error propagation from one FU (level *i*) to another FU (level *i+1*) that receives service from FU level *i* (i.e., external propagation) occurs when, through internal propagation, an error reaches the service interface of FU level *i*. At this time, service delivered by FU level *i* to FU level *i+1* becomes incorrect, and the ensuing failure of FU level *i* appears as an external fault to FU level *i+1* and propagates the error into FU level *i+1*.

3. A failure occurs when an error is propagated to the service interface and unacceptably alters the service delivered by the system. A failure of a FU causes a permanent or transient fault in the system that contains the FU. Failure of a system causes a permanent or transient external fault for the other system(s) that interact with the given system.

These mechanisms enable the 'fundamental chain' to be completed, as indicated by Figure 3.

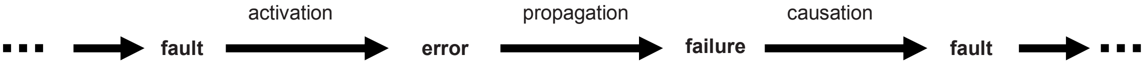


Figure 3 – Example for the mechanisms of 'fundamental chain'

From a time domain point of view the failures can be classified in "permanent" or in "temporary" depending on the activation patterns conditions.

Whatever the creation mechanism or the time domain class is it, in the following sections reference will be done to "failures" classified into "systematic" and "random" characteristics.

Figure 4 shows a practical example of the relationship between external events, components faults, errors and other failures which could lead to hazards with respect to system- or sub-system hazards.

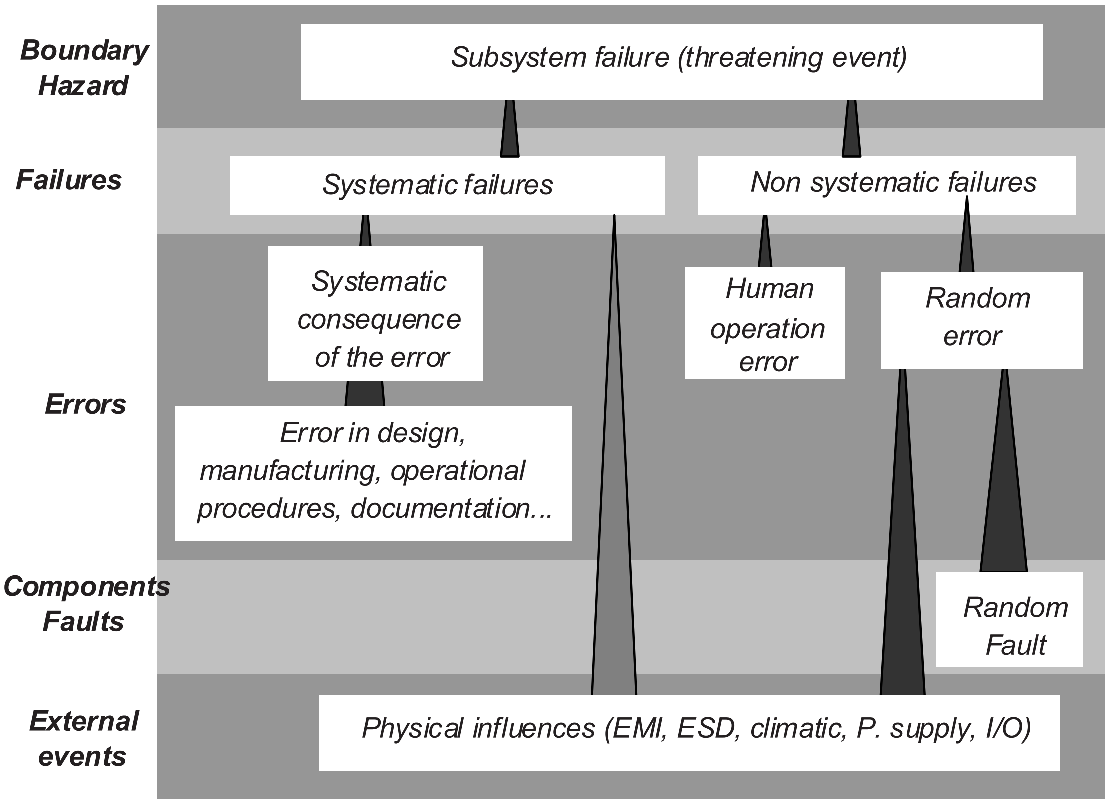

Boundary Hazard
Subsystem failure (threatening event)
Failures
Systematic failures
Non systematic failures
Errors
Systematic consequence of the error
Human operation error
Random error
Error in design, manufacturing, operational procedures, documentation...
Components Faults
Random Fault
External events
Physical influences (EMI, ESD, climatic, P. supply, I/O)

Figure 4 – Relationships of faults, errors and failures

Systematic failures, are non quantifiable, but should be completely evaluated and extensively mitigated by the relevant process and technical measures.

Systematic failures can be induced by

- specification or design errors,
- pre-existing faults (SW design error, error on programmable device, etc.),

- manufacturing and hardware faults (procedure, error or use of wrong component material),
- tools faults (compiler, development tools, etc.),
- process (design, development, operation, etc.) or maintenance errors.

Random failures are caused by stochastic failure processes, and have to be taken into account in different modes according to the type of applied fail-safety as suggested in the following sections. In many cases, random failures are described by a failure rate.

In SIL 3/SIL 4 inherent fail-safety devices no single fault should induce hazardous consequences.

In composite and reactive fail safety devices all single faults have to be detected and negated without directly leading to a hazardous consequence and the combination of faults (with dormant faults or not) is to be evaluated.

There are special cases in which single faults can lead to a dangerous consequence but with a negligible probability. This case applies to coded monoprocessor and single channel data transmission where the redundancy/complexity of the information representation allows to detect all credible classes of physical failures in such a way that can be considered as a sort of inherent fail-safety.

- In coded monoprocessor techniques, the information operands and operators are coded in such a way that all possible classes of physical failures result in an information output able to self-reveal the errors and allowing an external negation reaction.
- In single channel data transmission, data are protected at the source for possible communications threats through specific techniques as specified in EN 50159-1 and EN 50159-2 allowing error detection at the receiver end.

Human operational errors should not be included in technical subsystem failures evaluation. If it is necessary to include them at system level, then they should be evaluated on a conservative basis and/or exported as a constraint for the upper level application. Currently, their quantification is not recommended due to the lack of related applicable standards.

4.1.2 External Influences and common causes as related to random and systematic failures

This subclause is in line with of EN 50129:2003, 5.4 and in particular with Section 3 “Effects of Faults” and Section 4 “Operation with External Influences” (see also EN 50129:2003, Clauses B.3 and B.4). This subclause gives more explanations and details on the relationship between random and systematic failures and their possible causes, influences or common causes.

Although systematic and random failures being of different natures, it may be considered that any one of them may correspond to a common cause or to external influences. Also, external influences inducing either systematic or random faults may correspond or not to common causes.

Figure 5 presents all possible cases and is followed by a table giving examples for all possible cases (Table 1).

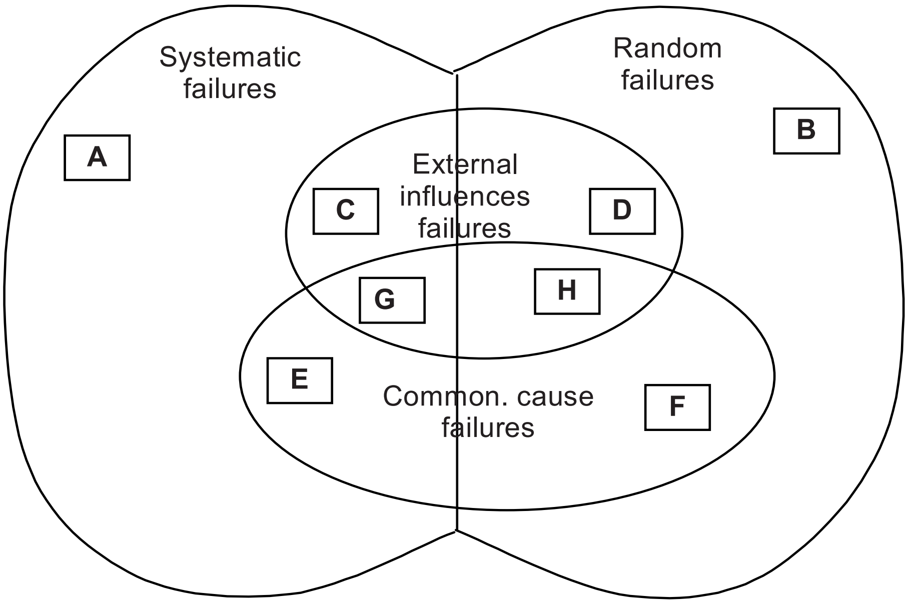


Figure 5 – Representation for failures of single and multiple natures

Table 1 – Examples for single and coupled failures types

Ref.	Main type	Specific cause or type	Examples (causes)	Fail-safety type
A	Systematic	---------	Subsystem specification or validation error	All
B	Random	---------	Single and/or multiple HW component fault	All
C	Systematic	Influences (int. or ext.)	EM pulse triggers fault in weak component	All
D	Random	Influences (int. or ext.)	EM pulse induces wrong SW computation	All
E	Systematic	Common cause	Compiler error in double channel; design error in voter (or reactive device)	Composite
F	Random	Common cause	Fault and dormant fault combination in double channels	Composite
G	Systematic	Influences and common cause	EM pulse induces wrong SW computation (or same HW fault in RAMs) in double channels	Composite and reactive
H	Random	Influences and common cause	EM pulse induces HW fault in voter (or reactive device)	Composite and reactive

It has to be noted that this has to be applied to all three types of fail-safety in different ways. The following non-exhaustive list for influences and common causes are given below:

a) internal influences:

- lack of galvanic insulation,
- electromagnetic coupling (cross-talk),
- common power supply perturbation,
- more details are given in EN 50129:2003, Clause D.3;

b) external influences:

- extreme temperatures,
- external power supply variations (over/under voltages, transients),
- conducted electric disturbances,
- radiated electromagnetic disturbances (including ionised radiation),
- chemical intrusion (if applicable),
- mechanical perturbations (vibrations and shocks),
- more details are given in EN 50129:2003, Clause D.3;

c) structural common causes:

- I/O structure common cause design error,
- inherent fail-safety fault in a voter device;

d) other common causes:

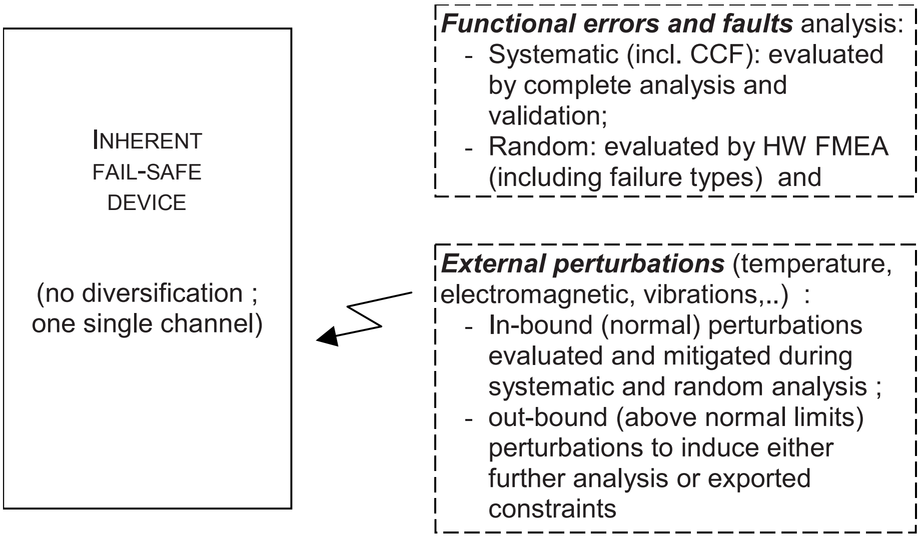
- compilers systematic design error,
- HW components (µP, Memory) systematic errors,
- etc.

EN 50121-4, EN 50125-1, EN 50125-2 and EN 50125-3 apply to external influences.

Subclauses 4.1.3 to 4.1.6 present application in every case with suggested mitigation presentation examples.

4.1.3 Application to inherent fail-safety

Inherent fail-safe devices may correspond to input/output interfaces or voting and/or inhibition (“passivation”) devices associated to composite or reactive safety based sub-systems (Figure 6).


INHERENT FAIL-SAFE DEVICE
(no diversification ; one single channel)

Functional errors and faults analysis:
- Systematic (incl. CCF): evaluated by complete analysis and validation;
- Random: evaluated by HW FMEA (including failure types) and

External perturbations (temperature, electromagnetic, vibrations,..) :
- In-bound (normal) perturbations evaluated and mitigated during systematic and random analysis ;
- out-bound (above normal limits) perturbations to induce either further analysis or exported constraints

Figure 6 – Inherent fail safe devices structure and associated threats

Table 2 suggests the associated mitigation measures.

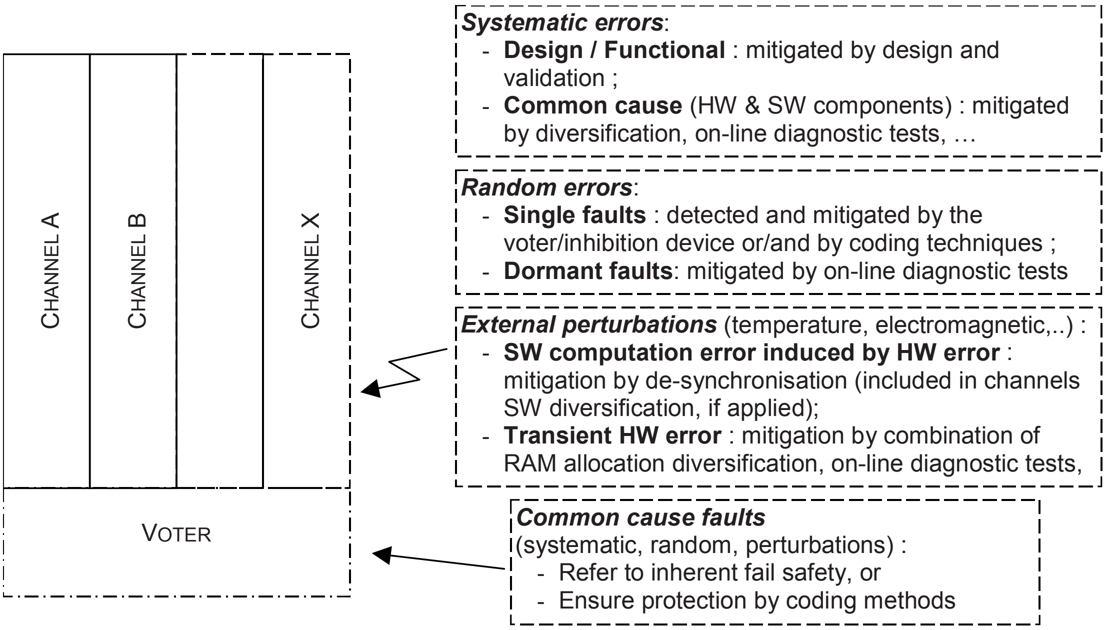
Table 2 – Guidance for threats mitigation in inherent fail-safe devices

Failure type	Causes / Faults / Errors	Mitigation / Protection means
Systematic – functional	- Design error; - CCF; - HW Component systematic error (misuse, wrong replacement...); - In SIL 4 design should include protection against components random single faults and in SIL 3/SIL 4 possible combination of faults.	- Skilled State of the art design, and validation process under Quality Control. - Skilled State of the art manufacturing and maintenance processes under Quality Control. - In SIL 3/SIL 4 applications FMEA (and FTA) should analyse single and multiple faults effects.
Random	- Components random fault	- FMEA and failure tests (with all types of possible component failure). - In SIL 3/SIL 4 applications FMEA (and FTA) should analyse single and multiple faults effects. - For serial I/O: protection by Coding techniques.
Random – in-bound external perturbation	- Component induced faults; - Induced wrong behaviour.	- FMEA and tests should include maximum forecasted external perturbations. - Validation process should include specified level of acceptable perturbations.
Random – abnormal external perturbation	- Component induced faults; - Induced wrong behaviour; - Abnormal handling or operation of the device (wrong input for instance).	- Export constraints on abnormal operation/handling of the device. - Export constraints on perturbation levels. - If applicable: specific evaluation on abnormal external perturbations.

4.1.4 Application to composite fail-safety

Composite fail-safety is implemented by multi-channelling. In railway application are normally used the 2oo2 (two out of two) and 2oo3 (two out of three) structures.

These structures may be implemented with a common device ensuring the vote and the inhibition of failed channels, which at least partially has the properties of an inherent fail-safe device and is to be evaluated accordingly (Figure 7). Alternatively voters may be used in every channel.



Systematic errors:
- **Design / Functional** : mitigated by design and validation ;
- **Common cause** (HW & SW components) : mitigated by diversification, on-line diagnostic tests, …

Random errors:
- **Single faults** : detected and mitigated by the voter/inhibition device or/and by coding techniques ;
- **Dormant faults**: mitigated by on-line diagnostic tests

External perturbations (temperature, electromagnetic,..) :
- **SW computation error induced by HW error** : mitigation by de-synchronisation (included in channels SW diversification, if applied);
- **Transient HW error** : mitigation by combination of RAM allocation diversification, on-line diagnostic tests,

Common cause faults
(systematic, random, perturbations) :
- Refer to inherent fail safety, or
- Ensure protection by coding methods

Figure 7 – Composite fail safe devices structure and associated threats

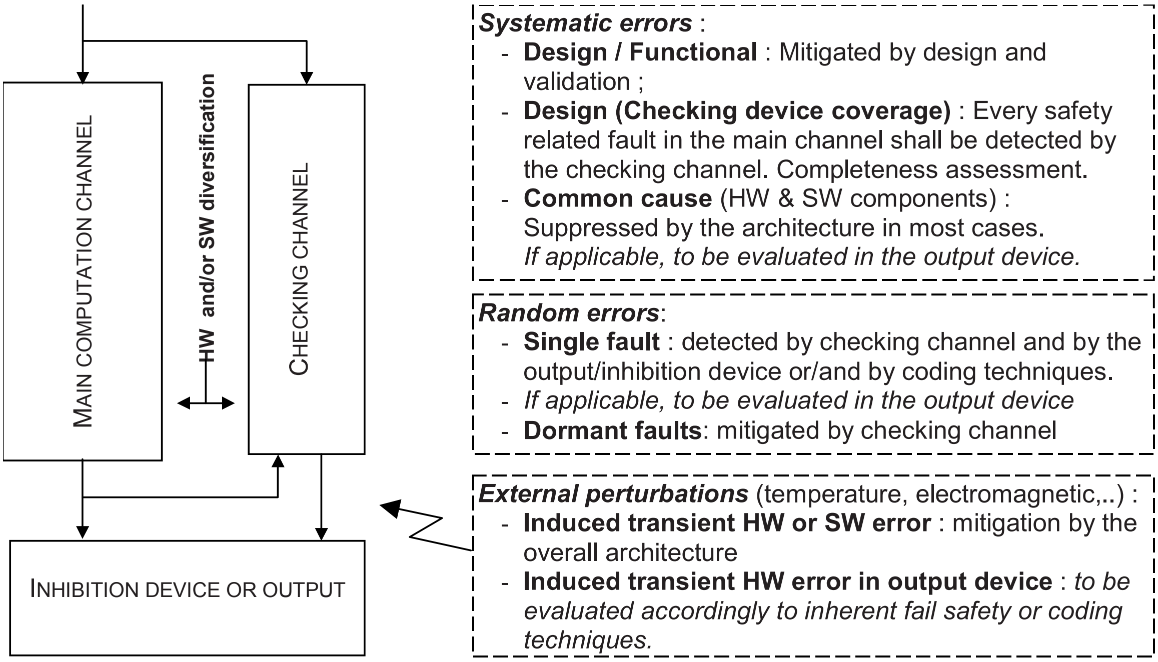
Table 3 is non exhaustive and suggests the associated mitigation description.

Table 3 – Guidance for threats mitigation in composite fail-safe devices

Failure type	Causes / Faults / Errors	Mitigation / Protection means
Systematic	Subsystem / SW specification, design or validation error	- Skilled State of the art design and compliance with standards and validation processes under Quality Control.
Random	Single HW component fault	- Voter, inhibition and/or coding techniques.
Systematic - Common cause -	Compiler error in multiple channels	- Compiler validation, or - SW or compiler diversification.
	Use of same HW bugged (same manufactured series) or ageing devices in multiple channels	- Online Tests (on µP or Memory), or - Specific coding techniques, or - HW diversification, etc.
Random - Common cause -	Double HW component fault (including a dormant fault)	- Online Tests (associated to coverage and evaluation on Fault disclosure Time).
Systematic - Induced by perturbation - (particular common cause)	EM pulse induces same HW error in devices with marginal characteristics	The systematic classification of the event is a marginal characteristic. To deal with is the below guidance also applicable.
Random - Induced by perturbation - (particular common cause)	EM pulse induces wrong SW execution	- Qualification according to relevant parts of EN 50121 series - De-synchronisation between any two channels (already performed in case of SW diversification).
	EM pulse induces same HW error in identical components (i.e. in data Memory) in multiple channels	- Qualification according to relevant parts of EN 50121 series - HW diversification, or - Data mapping diversification in the Memory of the multiple channels.
NOTE This table is not to be considered as exhaustive. Depending on every case other causes should be taken into account (for instance: internal electric perturbations, temperature drifts, vibrations, events in programmable devices, etc.).		

4.1.5 Application to reactive fail-safety

Reactive fail-safe devices implement either SW diversification or most frequently both HW and SW diversification. This architecture by itself mitigates some threats taken into account in the composite architecture. The reaction time however is to be specifically evaluated. See Figure 8.



Systematic errors :

- **Design / Functional** : Mitigated by design and validation ;
- **Design (Checking device coverage)** : Every safety related fault in the main channel shall be detected by the checking channel. Completeness assessment.
- **Common cause** (HW & SW components) : Suppressed by the architecture in most cases. *If applicable, to be evaluated in the output device.*

Random errors:

- **Single fault** : detected by checking channel and by the output/inhibition device or/and by coding techniques.
- *If applicable, to be evaluated in the output device*
- **Dormant faults**: mitigated by checking channel

External perturbations (temperature, electromagnetic,..) :

- **Induced transient HW or SW error** : mitigation by the overall architecture
- **Induced transient HW error in output device** : *to be evaluated accordingly to inherent fail safety or coding techniques.*

Figure 8 – Reactive fail safe devices structure and associated threats

Table 4 suggests the associated mitigation measures. The common cause classification is not used as there are no multiple common functions concurrently performed.

Table 4 – Guidance for threats mitigation in reactive fail-safe devices

Failure type	Causes / Faults / Errors	Mitigation / Protection means
Systematic	Subsystem / SW specification, design or validation error	- Skilled State of the art design and validation process under Quality Control
	Non coverage by the checking device of all main device safety related functions	- Coverage completeness validation by tests and safety analysis.
	Output/inhibition device time reaction increase or discrepancy.	- Time reaction application suitability (exported constraint or other); - Validation by analysis and test of the inhibition principle and delay.
Random	Single or multiple HW component fault	(inherently mitigated by the architecture in main and checking channels). - Voter, inhibition and/or coding techniques in the output / inhibition device.
Systematic or Random - Induced by perturbation -	EM pulse induces wrong SW execution or transient HW error	Qualification according to relevant parts of EN 50121 series - (inherently mitigated by the architecture).
	EM pulse induces same HW error in output/inhibition device	- Qualification according to relevant parts of EN 50121 series - Inherent fail-safety technique, or - Coding technique.
NOTE As in previous subsections the above items should be completed depending on the specific implementation.		

4.1.6 Example of safety principles justification

The safety principles as presented above correspond to the mitigation of safety threats and are in correspondence with EN 50129:2003, 5.4 and Clause B.3. As such, this provides guidance for related justification in the corresponding sections of a Safety Case.

In the particular case of product platforms, including the HW with its associated SW kernel part, it is considered as good practice to have a separate technical and safety document, the so called “Justification of Technical Safety Principles” or “Safety Concept”, which is referred to by the Safety Case. This is often interesting because it mainly deals with technical issues related to functions implementation rather than with the functional safety issues. It has proved in the past experience to be a tool to detect and mitigate safety issues in the early stages of such platforms development.

The proposed structure for such Safety Principles document could include

- its aim, contents and definition of faults, errors, failures and hazards,
- analysis tables focusing on systematic, random and common cause failures identification and association with related requirements and mitigation measures. These analyses are performed according to a bottom-up (inductive or FMEA like) analysis starting on components/parts faults,
- information from the above analysis should be consolidated in a synthesis table associating every error or failure to the corresponding mitigation measures. Mitigation measures are translated in requirements which have to be closed by the on-going product development or imported/exported from/to the upper/lower level application level,
- another part of the document could be dedicated, when applicable, to quantifiable errors and failure computation. A top-down analysis (FTA) or a Markov calculation could be allocated to every identified hazard.

This document should be considered as corresponding to an iterative process together with product's specification and architecture in the early stages of the development process. This iterative process is complete when systematic faults/errors are fully evaluated as mitigated and the quantitative estimation of the global Wrong Side failure rate is acceptable.

The development requirements issued by this analysis may be supplementary to those that may be imported from higher-level subsystem/system safety analysis.

4.2 Components development guideline

EN 50129:2003, Annex C, deals with “Identification of hardware component failure modes”.

Hardware components can be split in two major parts: Components with Inherent Physical Properties, and Programmable Components or Devices.

Subclause 4.2.1 gives explanations on how to achieve failure modes analysis on components with Inherent Physical Properties by means of simulation and theoretical justification in order to disclose all the hazardous failure modes.

Subclause 4.2.2 gives examples and explanations on different fail-safety architectures (composite or reactive) using Programmable Components, or devices, such as VLSI (FPGA, EPLD...) with guidance for their development.

Subclause 4.3 presents other implementation examples together with the conditions these components should satisfy to be included in a safety design.

4.2.1 Components with Inherent Physical Properties

For a great number of electronic components (e.g., inductor, transformer, diode, transistor, relay, mechanical resonator, etc.), it is often difficult, or even impossible, to realise physically, the different failure modes (e.g., short-circuit between turns of a winding, increase or decrease of inductance, increase or decrease of conducting state voltage, increase or decrease of DC or AC amplification, contact chatter, increase or decrease of Q-factor, etc.).

In that case, and as described in the first paragraph of EN 50129:2003, Clause C.4, simulation can be used as a complement to the normal HW FMECA and related laboratory failure tests. The evidence of the inherent physical properties working towards or against the safety and related to the tool simulation should be provided in attachment, either by theoretical explanation or by simulation of well known past cases (proven in use character). The results of the simulation tests themselves are included in the main HW FMECA as part of the HW safety Analysis.

This complementary simulation activity, when implemented, should allow together with the classical failure mode tests and analysis to provide a restricted (in any case smaller) set of residual failures to be justified by analysis.

The simulation could be done on a computer by means of particular simulation software packages. The simulation results should be recorded in a companion report or as an attachment to the main HW safety analysis report. It should contain the following elements:

- information for the simulation acceptance;
- results of the simulation;
- component models chosen for simulation and their parameters;
- environmental parameter variations (e.g. temperature, power supplies, electromagnetic disturbances, etc.);
- worst case analysis;
- random analysis (Monte-Carlo);
- version of the simulation software;
- complete references of the testing computer (type of operating system and relevant software version numbers, configuration);
- skills of the operator(s).

The simulation Tool should be either proven in use or qualified by internal and/or external evaluation/assessment.

4.2.2 Programmable devices safety development (SIL 3 and SIL 4)

For programmable devices (e.g. VLSI, FPGA, PAL and ASIC) including SIL 3 and SIL 4 parts, protections should be implemented in the design.

In accordance with EN 50129:2003, Clause C.3, it is very difficult, or even impossible, to predict all the failure modes of very large scale integration components such as integrated circuits, FPGA, EPLD, microprocessors.

As a matter of fact, if we know the functional architecture and the electrical operation of such components, we really do not know the internal architecture (e.g. proximity of the tracks, feeders of common power supplies, etc.), so it is difficult to predict all their different failure modes. Furthermore the internal design of this kind of components can be changed, at any time, by the supplier without any information to the customers.

As a consequence of the complexity of Very Large Scale Integration it is generally considered as impossible to define failure scenarios and to ensure 100 % of coverage rate with Online Tests implementation.

The implementation of safety related functions in such devices implies special care, using composite or reactive fail-safe techniques or data transmission coding strategy protection related techniques.

Examples of acceptable designs are described in 4.2.2.1 to 4.2.2.6, with indication of the related constraints whenever applicable.

4.2.2.1 Use of single device without redundancy:

There are at least two possible cases:

1) the processed information is protected by a code and a date. All internal device errors on dynamically protected data are to be detected by external receivers or controllers featuring SIL 3 or SIL 4 characteristics. The corresponding evidence of safety should comply with EN 50159-1. The failure rate corresponds to the used Coding Strategy by taking into account all applicable perturbations and failures;

2) two different and diversified paths may be designed in the same device. The diversification can be ensured by different information structure (registers and serial message for instance), by diversified VHDL (positive and negative logic, etc.), different algorithms, or by any other convenient means with its associated safety justification. In this case refer also to the design remarks presented hereafter for two identical devices.

4.2.2.2 Use of two identical devices in a redundancy arrangement

The most general structure is shown in Figure 9, which includes alternative possible features (generally only part of them is implemented, and others may even be possible). Inputs may be or not common to both devices.

Other structures as 2oo3 are also possible, with identical design principles and proof of safety.

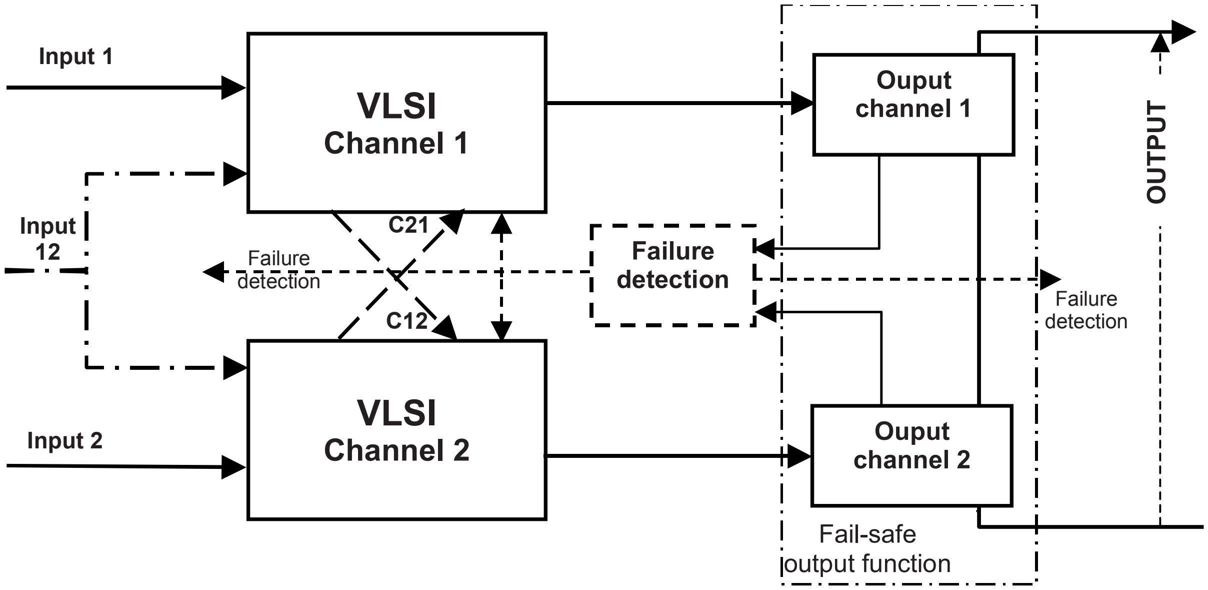


Figure 9 – Example of composite fail-safety with identical VLSI components

In relation with the safety design some points among the following should be considered:

- diversification could be implemented, as far as possible, to ensure mitigation against systematic and common cause failures:
  - the VHDL (or other) code could be diversified by using different programmers or different algorithms,
  - it is recommended to introduce a partial HW diversification by having complementary logic status in all or part of the inputs and outputs. In the same way choosing a different pin out for the two devices also enforces the proof of safety,
  - another possibility is to have different information structure in the two channels; for instance, serial coded information in one channel and the same information in parallel registers in the other channel;
- connections c12 and/or c21, if implemented should not be prone to introduce common cause failures. For instance, the transit information is coded with a key not known by the outside receiver (external device receiving the information), for use on its final computation;
- periodic diagnosis tests should be implemented when other means are insufficient, which generally induces the implementation of a failure detection circuit. This detection device may be implemented on the nearby vicinity (as in the above figure, where it picks up data in the outputs interfaces) or in the outside receiver; but in all cases it detects the failure in channel 1 or in channel 2. As shown in the figure, its blocking action may take place upstream, downstream or in the VLSIs themselves. In some cases the outside receiver blocks itself in the restrictive state;
- the fail-safe output mechanism or device may be implemented either by means of an inherent fail-safety device or by superposition of encoded data (the corresponding Coding Strategy providing then an acceptable protection level).

4.2.2.3 Use of two different devices in a redundancy arrangement

The possible cases correspond either to composite or to reactive fail-safety:

- in case of different devices implementing identical functions (composite fail-safety) the same constraints as above apply. The global evidence of safety could be simplified by the argument of HW diversification (which could, alone, induce SW diversification);
- having different functions implemented in the two devices is generally related to the implementation of a reactive fail-safety strategy. As in the example shown in Figure 10, the computation carried out in one device (“main”) follows a coding strategy in its input data, which only the second device (“reactive”) is able to understand or/and to re-inject in the initial input data. The second device de-scrambles the final data and provides the final output with the safety level ensured by the corresponding Coding Strategy.

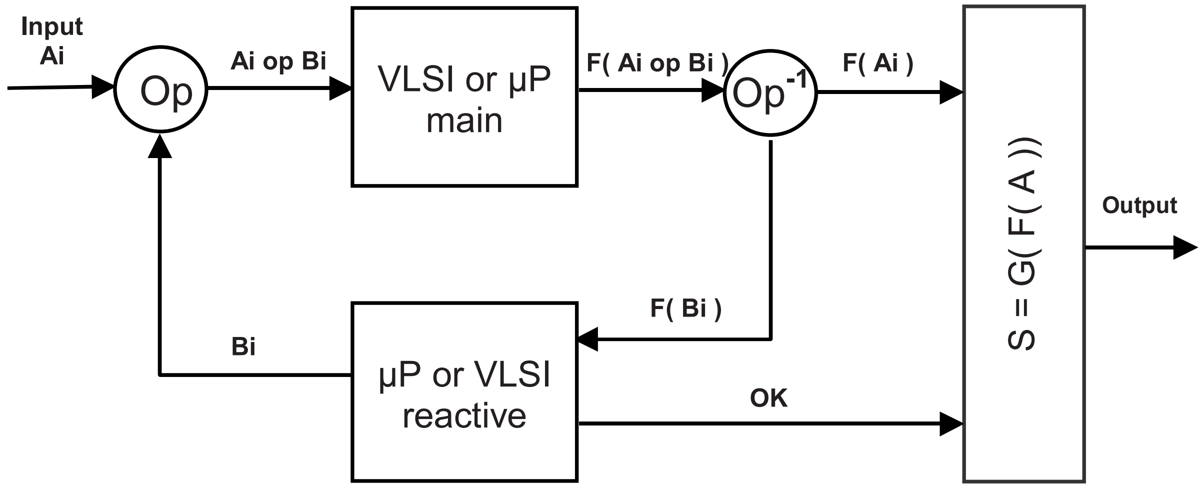


Figure 10 – Example of reactive fail-safety with different VLSI components

4.2.2.4 Safety integrity level allocation

The safety integrity level allocations to these VLSI (or for the related functions) are done at the upper component level (Board for instance). For quantifiable (non systematic) failures the partial failure rate of the VLSI components is part of the upper level component failure rate (both for all and for safety related faults).

SIL 3/SIL 4 constraints will apply identically for the related development process as related to hazards coming from non-quantifiable systematic failures.

4.2.2.5 Safety Evidence

For all cases in this section, safety evidence should be produced to demonstrate that design features cover all identified threats. Subclause 5.1 should be of some help on doing so.

Some particular points are suggested hereafter in order to complete the provision of safety evidence in relation with the corresponding implemented design features: compliance with the applicable standards for creepage and clearance distances (EN 50124-1 or customer rules and/or requirements) or electrical connections requirements required on electronic equipment used on rolling stock (EN 50155):

- mitigation provided by HW or SW diversification implementation, if applicable;
- layout and routing files analysis should be added to the proof of safety folder whenever HW diversification is claimed for;
- justification of mitigation against systematic failures, common cause failures and double / dormant failures by means of one or several FMEA;
- evaluation of Diagnostic Tests (on line tests) coverage and justification of Diagnostic Tests intervals in relation with the related threats (to take into account the fact that 100 % coverage is impossible except in very simple cases);
- alternative methods like fault injection may be used to complete the proof of safety. Fault injection, if applied and to be taken into account in the proof, is to be characterised by its coverage rate. A 100 % coverage range can only be attained in simple configuration cases.

4.2.2.6 Suggested Programmable Components development and validation process

Considering that VHDL like developments will be from now on currently used, development and validation processes should follow the EN 50128:2001 and its Annexes as far as practically possible. Full compatibility (mainly related to phases sequencing) is generally not possible due to the fact that some operations are performed in different order comparatively to the normal cycle defined in EN 50128. Figure 11 below gives such an example.

Comparing with EN 50128:2001, Figure 4, it appears that the low part of the V-cycle (SW architecture & Design Phase, Code Phase, SW Module Design Phase, SW Module Testing Phase, SW Integration Phase) has a good correspondence of VHDL development, whereas the upper part (SW Requirements Spec Phase, SW/HW Integration Phase, SW Validation Phase) is in correspondence with the design and validation activity at the board level.

Phases and operations as defined in EN 50128 should have equivalent activities and document reports in relation with the apportioned SIL both at board level and at VHDL level. This correspondence should be clearly traced in final board safety report.

In relation with development phases it is also to note that all VLSI component design documents and intermediate files will join the Board documents in a normal configuration management process in order to allow possible design evolution and future inspection.

Moreover, some complementary documented activities are to be performed as the VLSI component also interferes as an HW component. In particular, its pin out configuration is to be evaluated jointly with barriers separation in the Board HW safety analysis.

An important remark may be added concerning the maintenance phase. In case of SW rework regression tests are not to be only partially done but completely performed as there can be no complete traceability against the cells location in the VLSI component. In fact, the design and validation process would better be entirely automated in order to allow easy design evolution.

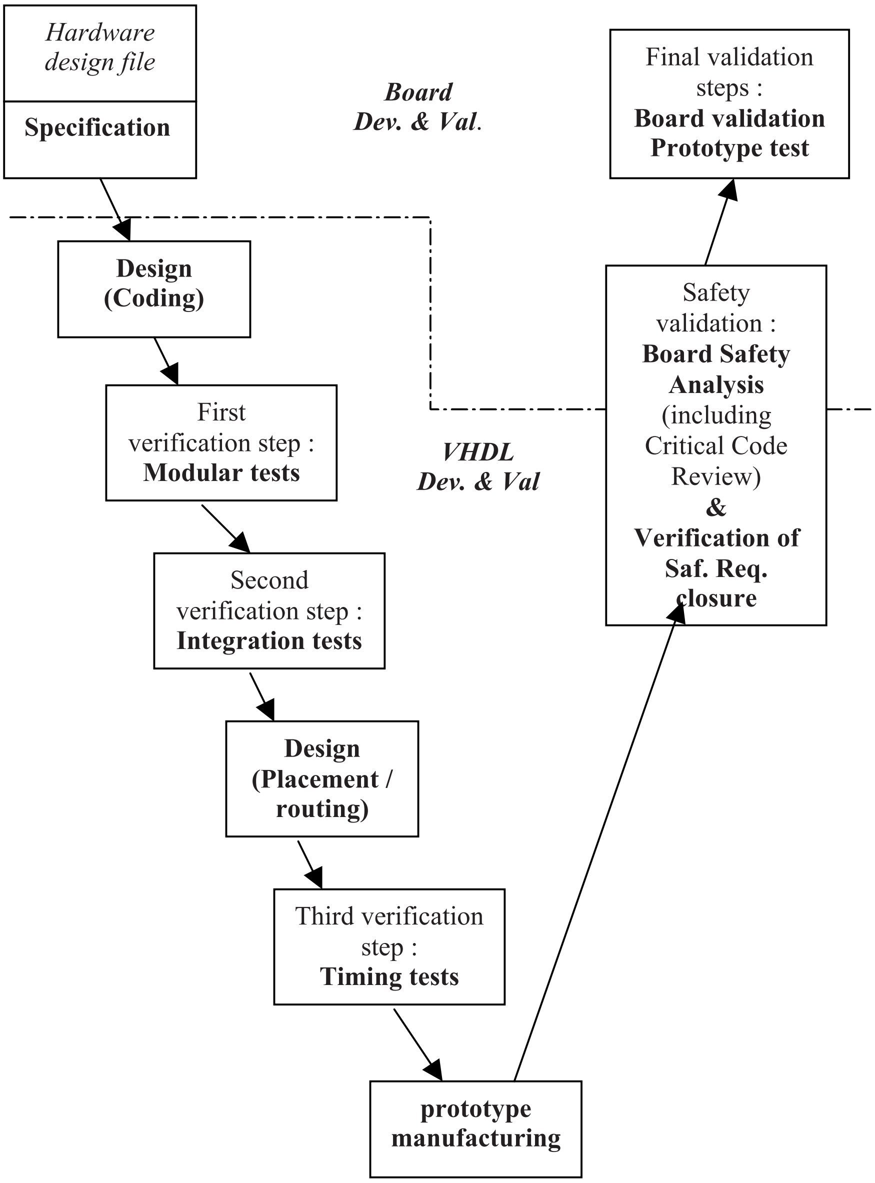

Hardware design file
Specification
Board Dev. & Val.
Final validation steps : Board validation Prototype test
Design (Coding)
Safety validation : Board Safety Analysis (including Critical Code Review) & Verification of Saf. Req. closure
First verification step : Modular tests
VHDL Dev. & Val
Second verification step : Integration tests
Design (Placement / routing)
Third verification step : Timing tests
prototype manufacturing

Figure 11 – Example of development process for VLSI components (FPGA, EPLD, etc.)

4.3 Specific implementation examples

Some examples are added presenting the state of the art.

4.3.1 Microprocessors and Microcontrollers

The safety evaluation has to be performed in two different levels:

- the mechanical level related to the associated technology and to the impact in its neighbourhood. As an HW component it has to be considered as SIL 0, but it can induce safety or reliability related constraints:
  - components pins technological soldering and mounting constraints,
  - use of multilayer PCB inducing possible threats to be mitigated near other components,
  - creepage and clearance distances constraints related to the above (between components and isolated group of components);

- the use of the component itself in a safety application. The following points have to be taken into account:
  - such a component, being SIL 0 has to be included in a composite (2oo2, 2oo3, etc.) or reactive (independent reaction device or coded programming) fail-safe structure,
  - whatever the structure only serial messages protected by approved coding strategies should be used. All exceptions should be justified (diversification, separation, complementary logic associated to inherent fail-safe AND function, etc.),
  - sequence and time validity in a function or algorithm computation. This means that at some level a SW safety analysis has to be performed, focused on possible internal component's function misuse or error (for instance, time reversed computations due to cache use, undue DMA use, etc.),
  - mitigation according to described safety principles for systematic errors related to components and compilers.

4.3.2 Sensors

Sensors, always related to inputs, may be categorised in two groups, the first related to dynamic data (speed and incremental encoders) and the second to discrete inputs capture.

4.3.2.1 Use of dynamic (fast changing) input sensors (speed and incremental encoders)

Those sensors have generally multiple outputs which can be either digital or analogue. In both cases a composite or reactive fail-safe strategy has to be implemented as no single channel can be designed to ensure inherent fail-safety.

The corresponding composite or reactive structure should be evaluated according to previous described “safety principles” methods with some highlighted particular points:

- the channels should not present non evaluated possible common errors causes from the sensor end (power supply for instance) to the final computation end;

- the diversification level (HW or/and SW) has to be chosen accordingly to the corresponding allocated SIL and dully justified in the Technical Safety Report or in a referred document;

- in case of use of analogue to digital converters the common cause error possibility (temperature drift, for instance) should in most cases justify HW diversification;

- the information time validity is to be evaluated and justified, at least in SIL 3/SIL 4 levels. Of particular importance is the analysis of the possibility of wrong intermediate data memorisation;

- safety may be enhanced by the use of an HW or SW complementary device performing the continuous coherence between data in different channels, in complement to the final computation comparison.

4.3.2.2 Use of Discrete (slow changing or continuous) input sensors

Multiple design types are available. Among them two seem to be frequent:

- input implemented by means of independent dynamised (switched) sensors;

- use of a direct inherent fail-safety designed part combined to a specific input coded message generation.

The usual methods for inherent and composite fail-safety apply for these cases. In particular the above criteria for dynamic sensors also apply to the multiple input strategy.

Here a complementary point, which corresponds to the sensor threshold level has to be taken into account. The problem is naturally solved with speed and incremental encoders where the information is cyclically changing, whereas here the same logical state may stay for long periods. The safety evaluation has to include the analysis of the device or the strategy (commutation and sampling, periodic diagnosis tests, or others) implemented to mitigate threshold drifts.

4.3.3 Power Electronics

Motor drivers and power converters are out of the scope of Signalling equipment and so out of the scope of the EN 50129. However the boundary between signalling and power regulation/ braking is not so clear:

- emergency braking, service braking and speed regulation are directly bound to onboard ATP and ATC performances and safety levels. Overall signalling system analysis (power traction limitation, jerk limitation) may depend on RS (rolling stock) power regulation (now often SIL 2 designed) performances;
- the same transmissions network more and more interconnects on-board signalling and traction regulation functions.

It seems then acceptable for specific analysis to take into account traction/braking regulation performances and related safety levels.

Another point related to Power Electronics is the power supplies and power network structure.

Power supplies and power network structures should be evaluated accordingly to the following points:

- independence of the input power sources, for reliability, suppression of common cause failures, separation of perturbation paths, galvanic insulation between channels, etc.;
- mitigation against under and over voltage, transients behaviour (internally and externally generated), etc.;
- known and repetitive behaviour with overload, over (and under) temperature, etc.;
- acceptable transmitted electromagnetic perturbations.

4.3.4 COTS Components

Whenever used to perform safety related functions [3)] the use of COTS has to rely on described safety principles mainly applied to SW, but also with possible diversification in HW features. As an example one or several of the following mitigation elements should be applied, according to the required SIL level and related EN 50128 prescriptions:

- SW diversification in composite or complete HW and/or SW diversification in composite or reactive structures. A completely coded SW (including code instructions and data) is accepted in a single CPU board as a particular case of reactive fail-safety structure;
- inputs and outputs should only use serial links in association with a Coding Strategy;
- in a composite structure data fields should be diversified by means of location diversity in Memory, and generally in all memory devices as far as possible;
- in composite structures galvanic insulation should be considered between channels, and by so between COTS. In particular, they should be powered by independent and separated power supplies;
- periodic diagnosis testing;
- plausibility tests (e.g. checking Value, Range, Type, dimension, etc.);
- etc.

[3)] Here safety-related means SIL 3/SIL 4. For the SIL 1/SIL 2 levels, requirements on software defined in EN 50128 can be considered as sufficient.

5 Safety case structure in relation with associated documents and activities

5.1 Introduction

EN 50129:2003, Clause 5, defines how the conditions for safety acceptance and approval should be presented. The conditions should cover three headings:

- quality management;
- safety management;
- functional and technical safety.

The documentary evidence that these conditions have been satisfied should be included in a structured safety justification document known as Safety Case.

A key point for the provision of the necessary safety evidences for a project is the definition of a documentation plan that should be associated to the configuration of the delivered project. Guidance on the documentation plan is described in Annex B.

This subclause provides guidance on the content of the information addressed by the Safety Case document.

5.2 Safety Case for Signalling Systems

As prescribed by EN 50129, the Safety Case for a signalling system/subsystem/equipment is structured as follows:

- Part 1: Definition of System;
- Part 2: Quality Management Report;
- Part 3: Safety Management Report;
- Part 4: Technical Safety Report;
- Part 5: Related Safety Cases;
- Part 6: Conclusions.

The following subclauses provide guidance on these parts.

It is not unusual to have an annex to the Safety Case providing the project system documentation. The related documents are part of the list of the documents in Annex B.

The revision history of the safety case providing evidence of the evolutions should be handled in a release/version history subsection, generally belonging to Part 1.

NOTE The following guidance will introduce examples on key topics to be argumented inside the safety case. It is intended that a Safety Case document should not necessary describe exhaustively all the required information: as far as possible, it can limit the evidence to the applied rationale referencing other associated documentation (general procedures, specific project documentation, etc.).

5.2.1 Introduction and system definition structure

This introductory part of the Safety Case includes general issues and system description.

5.2.1.1 General Issues

This first part of Safety Cases (Clause 1) should include the following:

- purpose and scope sub-sections, including project/product context and applicability;
- definitions and acronyms. These may be presented in separate tables. Although reference may be done to an external document, the main related items are to be presented in this subclause;
- applicable and reference documents. Applicable and reference documents are of interest for the entire Safety Case document. Therefore this topic should be introduced in this section but then it should point to an annex to the overall Safety Case or a specific document listing all relevant references. This annex should include
  - applicable documents. Reference is made to the documents listed in this subsection (in a table for instance) and to their subsequent revisions. This list points, for instance, on Notice to proceed, Contract and relative annexes and any other applicable contract documents,
  - applicable legal requirements and standards. If reference is made to dated applicable standards, subsequent modifications and revisions to these will apply to this document only when expressly stated in a future revision of the same. For references to non-dated applicable standards, the last edition of the publication cited will be applicable. This list includes applied CENELEC standards, EN ISO 9001:2000, and others as internal procedures,
  - reference documents and standards. The reference documents and standards are cited in the text for a better understanding of the document and, in some cases, to provide additional information that is generally to be considered non-mandatory for applicability. This list includes Safety and Quality Manuals, internal application guides and related standards as EN 61508 series.

As good practise it is recommended to define a policy for controlling the configuration of the applicable and reference documents.

5.2.1.2 Overall system global structure

This section should present the general overall context to which the system / subsystem / equipment applies. The corresponding block-diagram is also to be shown.

In this case there is probably an embedded Safety Case structure that is also shown. Figure 12 applies to such a case.

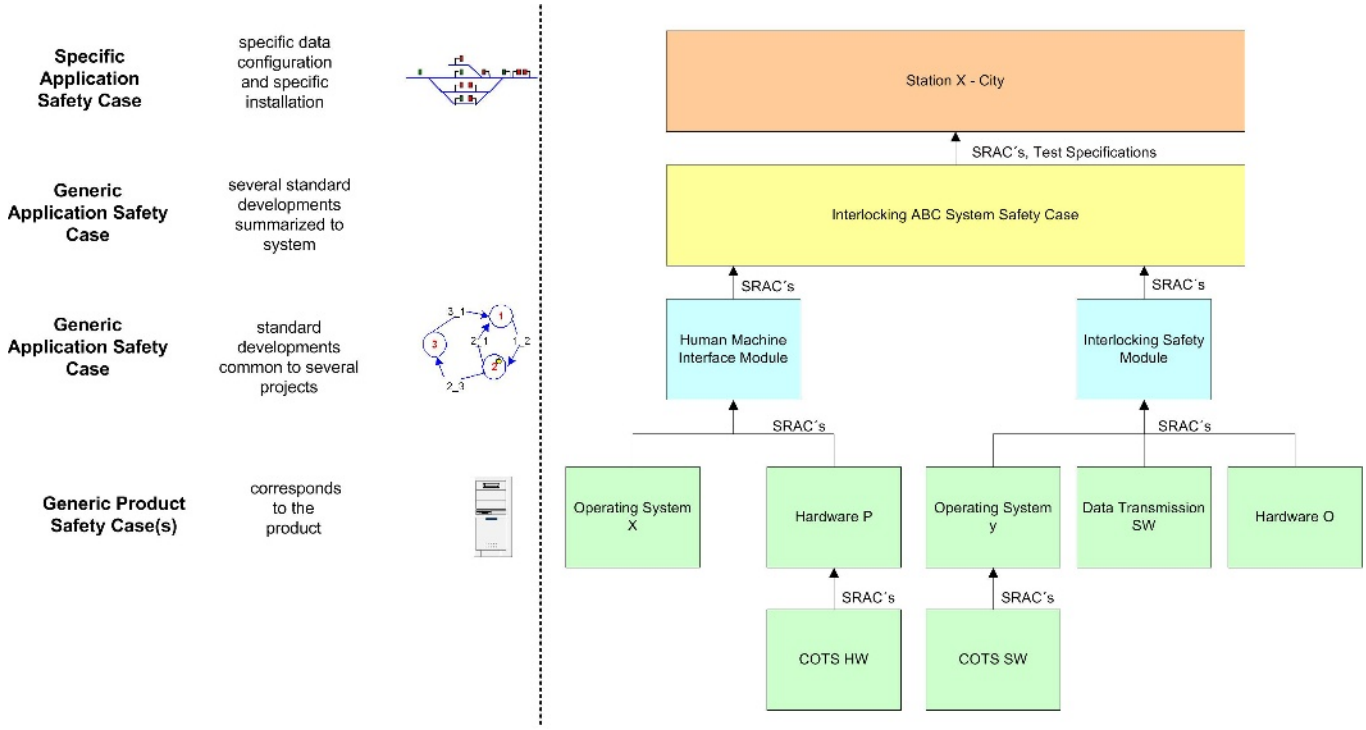

Specific Application Safety Case
specific data configuration and specific installation
Generic Application Safety Case
several standard developments summarized to system
Generic Application Safety Case
standard developments common to several projects
Generic Product Safety Case(s)
corresponds to the product
Station X - City
SRAC´s, Test Specifications
Interlocking ABC System Safety Case
SRAC´s
SRAC´s
Human Machine Interface Module
Interlocking Safety Module
SRAC´s
SRAC´s
Operating System X
Hardware P
Operating System y
Data Transmission SW
Hardware O
SRAC´s
SRAC´s
COTS HW
COTS SW

Figure 12 – Example of overall Safety Cases structure

Figure 12 provides a possible hierarchy of Safety Cases and related versioning:

- a Generic Product Safety Case addresses a core product used in Generic applications (e.g. Operating System, Core Computer System, etc.); they could possibly contain more supportive HW and SW COTS products;
- a Generic Application Safety Case addresses standard developments common to several projects;
- a Specific Application Safety Case addresses also specific data configuration and specific installation for a dedicated project.

Other configurations are also possible according to supplier best possibilities.

5.2.1.3 System description

This part of the introductory clause includes:

- definition of the System. This section should be fulfilled with the complete references of all system, subsystem and products versions to which the complete Safety Case applies. If applicable, mention has to be made on cross compliance between previous versions of component/sub-systems;
- overall description of the system. The overall description of the system could be a good practise according to the complexity of the safety case structure. Optionally this section could provide a description of the system/subsystem/equipment.

5.2.2 Quality management report structure

5.2.2.1 Introduction

Part 2 of the safety case provides evidence of Quality Management throughout the entire life cycle of the system under consideration.

The purpose of the Quality Management process is to minimise the incidence of systematic errors in every phase of the life cycle.

5.2.2.2 Quality System, Quality Plan and Quality Organisation

This section should present the Quality System and the related organisation.

The following points should be presented concerning the Quality System:

- relationship between the Organisation’s Quality System, which is normally applied by the Company, and the Quality Manual of the Organisation;
- organisation’s Quality System binding to all company personnel, as well as to the processes involved in the development, production, supply and the performance of assistance to customers;
- if applicable, approval of the Organisation's Quality System by a certification body (normally according to EN ISO 9001);
- periodicity of the Quality Assurance Department internal audits of each Company Department;
- revisions of the Quality System conditions under continued appropriateness, effectiveness and compliance with relevant ISO standards and with customer requirements. Define the management authorities in charge of these revisions. The revisions should include the certifications of the results of internal quality audits, the feedback from internal departments and from customers, and the monitoring of quality indicators. This information should be the input data to be used for updating company procedures and the Organisation's Quality Manual.

The approach to be applied to the Quality Management process for the System under consideration is described in the Quality Plan.

This document describes the planning carried out by the organisation for project development, production management and the installation of the System under consideration, and it also provides necessary details regarding the Organisation's aspects, specific quality procedures, resources employed, activities and schedules. The project Quality Plan should address the above points, plus the organisation structure and other points related to the evidence of Quality Management, internal and external audits as detailed in the following sections.

The Quality organisation should be presented in this section (or in another one specifically dedicated) by means of

- a block diagram presenting the Organisation from high level Management, until project Quality managers and engineers,
- a short task description for every Quality responsible, manager and engineer.

5.2.2.3 Evidence of Quality Management

The different aspects of Quality Management are covered by the documents listed in Table 5.

The items considered refer to the list in the Note contained in EN 50129:2003, 5.2.

Table 5 – Example of documentation linked to Quality Management

Aspects based on EN 50129:2003, 5.2	Examples of reference documents and/or Internal Organization's Procedures applied to the System under consideration
Organisational Structure	— Organization's Quality Manual — Quality Plans (QAP – Quality Assurance Plan)
Quality Planning and Procedures	— Quality Manual — Quality Plans (QAP – Quality Assurance Plan) — All other applicable Plans — Quality Records — Relevant Procedures Proc-1, …, Proc-n
Specification of Requirements	— System Requirement Specification (SRS) — Subsystem requirements specification (SSRS): — Apportionment of RAM and Safety requirements:
Design Control	— Design Plan
Design Verification and Design Reviews (Planning and Results)	— Design Plan — Formal Technical Inspection (FTI): Procedures and Reports
Application Engineering	— See Organisation's Quality Manual
Procurement	— Organisation's Quality Manual — Approval of Suppliers in the production of parts of the Product/System under Consideration — Quality Plans (QAP – Quality Assurance Plan)
Manufacturing	— Organisation's Quality Manual — Relevant Procedures Proc-1, …, Proc-n (see Note 1)
Product identification and traceability	— Configuration Management Plan (CMP) and -Procedures — Requirements Traceability Matrixes or equivalent methods
Handling and storage	— Organisation's Quality Manual — Relevant Procedures Proc-1, …, Proc-n
Inspection and testing (see Note 3)	— HW Test Specification — HW Test Report — Manufacturing, testing plans, factory tests — Type Tests — Type Test Reports
Non conformance and corrective actions (product-related)	— Organisation's Quality Manual — All reports regarding the results of test and check activities
Packaging and delivery	— Organisation's Quality Manual — Relevant Procedures Proc-1, …, Proc-n
Installation	— Installation, User and Maintenance Manual
Commissioning	— Organisation's Quality Manual — Relevant Procedures Proc-1, …, Proc-n
Operation and Maintenance	— Installation, User and Maintenance Manual

Table 5 – Example of documentation linked to Quality Management *(continued)*

Aspects based on EN 50129:2003, 5.2	**Examples of reference documents and/or Internal Organization's Procedures applied to the System under consideration**
Quality Monitoring and Feedback	— Corrective actions resulting from internal audits in the application of the Organisation's Quality Manual
	— Relevant Procedures Proc-1, …, Proc-n
Documentation and Records	— Relevant Procedures/Process — Evidence of Review Documents — Baseline Records
Configuration Management-Change Control	— Change Logs and Records — Relevant Procedures/Process — Baseline Records
Personnel Competency and Training	— Organisation's Quality Manual — Curriculum Vitae (CV) of all employees involved in the project — Technical knowledge acquired
Quality Audits and Follow up	— Quality Audit Protocols (NOTE 2)
Decommissioning and disposal	— Disposal of the System under consideration does not require any special precautions. The product does not contain dangerous materials that could contaminate the environment or cause damage to persons, animals or things — Reference: National Laws and EU Directives
Review of Quality Management System by Top Management ------------------------ Continuous Improvement	— Recording of the review of Quality Management System, including analyses and decisions regarding its improvement
Customer Satisfaction	— Analysis of received data on Customer satisfaction

NOTE 1 For instance, concerning PCB manufacturing, acceptability standard as IPC-A-610 could be referenced for safety related and safety critical products, and class 2 at least required.

NOTE 2 Audits and inspections are carried out internally, on sub-contractors and externally by third-parties as detailed in the following sections. An audit is a formal control, possibly based on checklists, to be performed on the process.

NOTE 3 An inspection is a formal control planned on specific lifecycle phases (material incoming inspection, factory acceptance tests, etc.) of the system/subsystem/equipment based on defined test specifications and procedures.

5.2.2.4 Quality audits and inspections

As part of the project, audits and inspections may be carried out

- with regard to the application of the operating procedures provided for in the contract documentation and in the reference standards by Customer or by Third Party Agencies (ISA),
- with respect to external suppliers or subcontractors. Since the responsibility of a supplier for products from a subcontractor is the same as that for their own products the same rules as below should apply to the subcontractor. The supplier and subcontractor should cooperate with the quality audits and inspections,
- by internal auditors.

The results of the quality assurance activities, quality audits and inspections may be summarised in a table highlighting the relevant issues from the reports of the different phases. Details concerning closed points should not necessarily be reported in this section.

Reference to existing reports should be made in this section.

Relevant results may be presented in the Internal Audit Report, in a table for instance, and state the following points:

1) item reference number;

2) reference for the audited process/action/report;

3) date of audit:

4) auditors;

5) findings description or audit comments;

6) status with criticality;

7) recommendations and remaining actions;

8) assessment of the mitigation for open points.

5.2.2.5 Summary and Conclusions on the Quality Management

The section should provide a final statement on the compliance of the Overall Quality Management System with the applicable standards.

A final synthesis should be presented on remaining actions, mitigation actions with a global summary.

This should conclude on the adequacy of the product or system being developed for the intended purpose.

5.2.3 Safety Management Report structure

As above, 5.2.3.1 to 5.2.3.13 provide either examples of contents (in italic characters) or lists of matters to be developed.

5.2.3.1 Introduction

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 50126-1,

- the organisational structure adopted complies with the EN 50129:2003, 5.3.3.

It also describes the activities carried out to guarantee the safety of the project in a manner which is consistent with the requirements of EN 50129.

The Safety Management methods, procedures and organisation applied for the project have been defined and documented starting from the preliminary project phases and specifically in the Safety Plan document.

5.2.3.2 Safety life cycle

It is to 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.

For example when different documents are summarized in one it can be justified that and why this was acceptable from the view of the safety management.

Note also that according to the project characteristics System/Subsystem/Equipment lifecycle phase may differ considerably which may lead to different contents in the table lines.

The Safety Management process is divided into a series of related phases and activities which make up the safety lifecycle, which is structured to be consistent with the system/subsystem/equipment lifecycle.

For the system/subsystem/equipment, the safety lifecycle has been divided into the phases listed in which highlights the relationship between the safety lifecycle phases and the system/subsystem/equipment lifecycle stages.

The lifecycle created is a V cycle, with the requirement specification, architecture and detailed design and development phases as top-down phases and the integration and validation phases as bottom-up phases. For each of these phases, the V&V activity required has been provided. For a detailed description of the lifecycle and the allocation of the various phases to this lifecycle (and for the relative HW and SW sub-cycles), and a description of the activities, refer to the Safety Plan (or other relevant plans).

This section should be in close relationship with EN 50129:2003, 5.4, Section 3 “Effect of Faults” of the Technical Safety Report. Specifically, in order to meet the requirements of that section, it should be provided argumentation on the following topics:

- reasonable selection of safety analysis methods applied at the different level of the project (system/subsystem/product);
- skilled execution of the chosen safety analysis.

The selection of the safety analysis methods and their combination based on EN 50129:2003, Table E.6, should be argumented based on the applicability for the Safety Integrity Level and the extent of the project.

For each phase of the system/subsystem/equipment lifecycle, specific safety analysis methods should be applied identifying the most efficient ones.

First of all, an association of the system/subsystem/equipment lifecycle phases to the Risk Analysis and Hazard Analysis tasks (see EN 50129) should be created.

A complete table listing the applicable phases of the lifecycle phases as defined in EN 50126-1 and related safety activities and safety documents should be provided based on Annex B.

Table 6 gives an example of deliverables related to the safety lifecycle activities, based on a simplified lifecycle as suggested by EN 50129:2003, Figure 5. Only documents supporting safety evidences are listed.

In case the project involves different hierarchical decomposition levels, e.g. system, subsystems, equipment, clear evidence of how the lifecycle phases are applied to each level should be provided.

An identification of the type of the project as “new development” or “modification/evolution”, could be useful to rank the safety activities that can be considered still applicable and the additional ones that need to be performed. In simple cases for modifications to the system/sub-system/equipment that do not change safety relevant properties of the concerned product, it is possible to proceed according to 6.3 in this Application Guide.

In the former case all the activities need to be carried out for the whole extension of the project, while in the latter case the analysis can remain confined to the modified parts, provided that justification of possible impact on the existing parts and strategy for non regression is argumented.

Table 6 – Typical Example of some Safety Activities in the Lifecycle

System/Subsystem/Equipment lifecycle phase	Safety lifecycle activity
System/Subsystem/Equipment Planning	Safety Planning and Safety Requirement Allocation: — Issue of the Safety Plan — Issue of the Documentation Plan, (may be included in the Safety Plan)
System/Subsystem/Equipment Requirements	Hazard Identification, Hazard Analysis and Risk Analysis, Safety Requirement Specification, Requirement Verification, Hazard Log Initialisation — Issue of the (Functional and Interface) Hazard Analysis or Preliminary Hazard Analysis (see EN 50129:2003, Annex E) — Issue of the Safety Requirement Specification, (included in the Subsystem Requirements Specification) — Issue of the Subsystem Requirements Verification Report
System/Subsystem/Equipment Architecture	Preliminary RAM Analysis, Hazard Analysis, Functional Test Definition, Architecture and Design Verification, continuation of Hazard Logging — Issue of the RAM Analysis — Issue of the (Architectural) Hazard Analysis with Safety Related Item List (SRIL)· — Issue of the Functional Test Plan — Issue of the Architecture Verification Report — Issue of the Hazard Log
	For HW: HW Requirement Verification, HW Safety Analysis, HW Failure Tests, HW Validation, continuation of Hazard Logging For SW: all activities according to EN 50128, continuation of Hazard Logging The set of documentation planned to cover the HW and SW design and implementation should be defined NOTE In particular it should be defined which document provides evidence of the traceability between software requirements identified during HW Safety Analysis and software documentation
System/Subsystem/Equipment Integration/Installation	Completion of RAM Analysis, Integration/Installation Test execution, Type Testing Definition and execution, continuation of Hazard Logging — Re-Issue of the RAM Analysis — Issue of the Type Test Plan — Issue of the Type Test Report — Issue of the Integration / Installation Test Report NOTE Installation Tests before Functional Validation could be not applicable when dealing with equipment level
System/Subsystem/Equipment Validation	Final Hazard Analysis, Validation, completion of Hazard Log, demonstration of Safety Level reached: — Issue of the Quantitative Safety Target Evaluation — Issue of the Hazard Log Report — Issue of the Functional Test Report / Validation Report — Issue of the Validation Report (including status of both functional and not functional requirements)

Methods for Safety Analysis: For each safety analysis task, a proper method should be selected and planned in the Safety Plan.

Table 7 provides guidance on the selection of the methods depending on the safety tasks: hazard identification and risk analysis (usually in the scope of railway authority), hazard analysis and safety demonstration (usually in the scope of the supplier).

Table 7 – Methods for Safety Analysis

Method	Hazard identification	Risk analysis	Hazard Analysis and Safety Demonstration (Safety Case)
ETA	Not applicable	Applicable	Possible
FMECA	Applicable	Applicable only for serial systems without redundancy	Applicable only for serial systems without redundancy
FTA	Not applicable	Possible	Applicable
HAZOP	Applicable	Not applicable	Not applicable
Markov	Not applicable	Applicable	Applicable
RBD	Not applicable	Not applicable	Applicable for non repairable systems
CCF analysis	Not applicable	Supporting	Supporting

The selection of appropriate methods needs to be done by joint effort of experts in safety and system engineering and a general guidance for a selection of one or more of the specific methods cannot be made. The selection should be done early in safety programme development and should be reviewed for applicability.

Table 8 proposes a list of safety methods and guidance for their level of applicability.

Table 8 – List of safety methods and reference Standards

Method	Suitable for complex systems	Suitable for novel system design	Quantitative analysis	Suitable for combination of faults	Suitable to handle sequence dependence	Bottom-up or top-down	Suitable for safety integrity allocation	Suitable for high safety requirements	Mastery required (from low to high)	Acceptance and commonality	Need for tool support	Plausibility checks	Availability of tools	Reference Standards
ETA	nr	nr	Yes	nr	Yes	B-U	nr	nr	High	avg	avg	Yes	avg	-
FMECA	nr	nr	Yes	No	No	B-U	nr	No	Low	High	Low	Yes	High	EN 60812
FTA	Yes	Yes	Yes	Yes	No	T-D	Yes	Yes	avg	High	avg	Yes	High	EN 61025
HAZOP	nr	nr	No	No	No	B-U	No	nr	Low	avg	Low	Yes	avg	IEC 61882
Markov	Yes	Yes	Yes	Yes	Yes	T-D	Yes	Yes	High	avg	High	No	avg	EN 61165
RBD	Yes	nr	Yes	Yes	No	T-D	Yes	nr	Low	avg	avg	Yes	avg	EN 61078

Key

nr = May be used for simple systems, not recommended as a stand-alone method, to be used jointly with other methods or with extra care
TD = Top-down
B-U = Bottom-up
avg = Average

5.2.3.3 Safety organisation

This section should report the details of the Safety Organisation established for the project according to EN 50129:2003, 5.3.3, optionally 5.3.9 and Table E.2. In this section of the Safety Management Report it should be reported that the safety management process is accomplished under control of a suitable organization. The degree of independence should be reported.

According to this the Safety organisation should be presented in this section by means of

— a block diagram presenting the Organisation from high level Management, until project Safety V&V and Project managers and engineers. In particular, the hierarchical and functional links between different acting people should be clearly shown, to provide evidence on the compliance to the above-referred standard sections,

— a short task description for every Safety and Project responsible, manager and engineer,

— the Safety organisation could also be described in a Development Plan, therefore a reference to the Development Plan may be suitable.

5.2.3.4 Safety Plan activities

This section in the Management report should provide evidence that the planned activities in the Safety Plan are fulfilled. The evidence may be presented in a tabular form with all safety activities listed from the safety plan and with reference to the corresponding documents carrying the evidence.

5.2.3.5 Hazard log

It is expected that several Hazard Logs may be created and managed on any system. The top level Integrated System Hazard Log records hazards identified via a top down hazard identification process and allows assignment (flow down) of safety requirements to sub-systems (owners of prevention, protection and/or mitigation safety requirements). When evidence of compliance to these flowed down requirements has been produced, reviewed and accepted, the particular hazard log entry may be ‘closed out’.

The Sub System Hazard Logs are used to record the identified causes of failing to meet sub-system safety requirements (hazards) and the evidence of management in the design, build, operation and maintenance of the technical system. The Sub-System Hazard Log should be supported by both a top down hazard identification process and a bottom up cause identification process such as FMEA.

Note that responsibilities for these different hazard logs may be with different organisations. In addition, processes should be in place to transfer relevant requirements between hazard logs, to ensure traceability and to define how these interfaces are managed. These interfaces have to be defined and agreed with all these parties and should be managed by the leader of the system integration.

The quality of a hazard log is not determined by the number of entries but rather the quality and sensibility of the analysis process used to determine hazard log entries.

A hazard log should be considered “live”. This means that the number of entries in a Hazard Log may grow throughout the life of the project (from Preliminary Design through to the end of the System’s serviceable life). Additionally, each entry of a Hazard Log should remain live. This means that an entry considered closed, due to receipt of design and build evidence, may be reopened if modifications are proposed or operational/maintenance evidence suggests that the risk resulting from the hazard is too high.

The hazard log consists of series of records. Hazard Log management can preferably be administrated in a SW-database and needs frequent update driven by the complexity of the system, sub-system or equipment. Management of hazards should be described completely and documented (the process for this handling has to be defined in the safety plan).

The Hazard Log should be initialized in the earlier phases of the safety lifecycle, at least after PHA or SHA during “system (or equivalent subsystem / product) requirement” phase as described in Table 2.

The current hazard status should be reported in the safety case and open hazards may result in safety-related application conditions.

The following should be reported:

- the methods, tools and techniques used;
- the personnel, and their competencies, involved in the process;
- the structure of the Hazard Log should be referenced.

As an example the following information can be used:

- unique identification number;
- date of the logging;
- originator;
- each hazardous event (brief description of the Hazard);
- components involved (affected system, sub-system or equipment with type and version);
- cross reference to the full description and analysis (including safety reviews and audits).
- likely consequences and frequencies of the sequence of events associated with each hazard;
- the risk of each hazard (the risk is defined as the product of the frequency or probability and the consequence of a specified hazardous event);
- the measures taken to reduce to a tolerable level, or remove, the risk for each hazardous event;
- a description of any analysis carried out, its limits, any assumptions made during it or any confidence limits applying to data used within it;
- status: open / cancelled / resolved (verified) / closed (validated).

This section of the Safety Management Report should include a summary on the current status of the Hazard Log with indication of the number of items in every defined class (open, resolved, closed, exported (application, operation, etc.) and total of registered points).

It is also necessary to include (here or in the Conclusions clause or with reference to a dedicated annex) a table or a straight presentation of all remaining open points with indication of

- criticality,
- remaining action for closure,
- existing mitigation measures,
- assessment on every remaining point.

5.2.3.6 System / Sub-system / Equipment Safety Requirements Specification

Evidence will be given either as this document exists or is realized as part of system requirements specification.

Safety Requirements should be specified at each phase in which a Requirements Specification is planned (system/subsystem/equipment).

According to what defined in the safety management process, safety requirements are usually identified in safety analysis (Risk Analysis, Hazard Analysis, etc.). The following cases apply:

- the identified safety requirements were already specified in the requirements specification. In this case a traceability should be provided;
- the identified safety requirements were not previously specified. In this case they represent new requirements to be added to the requirements specification.

This section of the safety case should provide reference to all the documents representing the collection of the safety requirements.

5.2.3.7 System / Sub-system / Equipment Design

The following text gives an example how the design documentation can be organised.

> The design phase of the system/subsystem equipment has produced the design documents covering the following topics:
>
> - System/subsystem/equipment Architecture Description;
> - Software Requirements Specification;
> - Hardware Requirements Specification;
> - Subsystem/equipment Type Test Plan.
>
> At the end of the design phase the verification activity has been carried out. The result of this activity was documented in the System/subsystem/equipment Architecture Verification Report providing the following results:
>
> - traceability of the requirements between System/subsystem/equipment Requirements Specification and design documentation;
> - top-down, structured design methodology for the architecture. Specify which Techniques/measures of EN 50129:2003, Table E.7 have been applied in accordance to the specified SIL level;
> - relationship between hardware and software according to EN 50128. Specify which Techniques / measures of EN 50128 have been applied in accordance to the specified SIL level;
> - list of environmental requirements and correspondence with Type Test Planning / Environmental studies. Specify the list of applied Standards / normative.

NOTE A specific analysis (FMEA for instance) should be performed at every level of Specification and Design in the top-down part of the V cycle System/Sub-System SW/HW development. This is necessary in order to implement mitigation against new risks/hazards that can be introduced by technical functions and specific solutions. It is highly recommended that Specification (and Design in some cases) document uses structured analysis tools (SADT, SART, etc.) in order to allow completeness of the related safety analysis.

5.2.3.8 Safety Reviews / Safety Audits

5.2.3.8.1 Safety Reviews

This section of the Safety Management Report covers the state of the activities set up following the Safety & Design Reviews generated by customer analysis and/or the internal analysis applicable, indicating the phase and the documents involved. In general all the technical requests should be accepted. If it is not the case, justification should be provided. The following aspects should be considered:

- item reference number;
- reference for the reviewed document;
- date of Review;
- reviewers;
- the phases of the life-cycle and documents reviewed;
- review comments;
- status of the recommendations and actions;
- assessment of the mitigation for open points.

A synthesis should be presented on remaining actions, mitigation actions concluding on the adequacy for the product or system being developed

5.2.3.8.2 Safety Audits

A Safety Audit is a systematic and independent examination to determine whether the procedures specific to the requirements of a product comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives. It serves therefore to achieve compliance of the management process with the safety plan.

If planned, external and/or internal safety audits can be held in order to analyse the safety management. These audits should document compliance to the EN 50126-1, EN 50128 and EN 50129 standards. In this case this section should report safety audits identifier, the associated report and the result or findings. The following items should be recorded as an output of the audit process:

- item reference number;
- reference for the audited subject;
- date of audit;
- the names and credentials of auditors;
- the phases of the life-cycle audited;
- audit observations and findings;
- status of the recommendations and actions;
- assessment of the mitigation for open points.

A synthesis should be presented on remaining actions, mitigation actions concluding on the adequacy for the product or system being developed.

5.2.3.8.3 Evolution/Modification Safety Reviews

Evolutions/modifications should be managed according to dedicated quality procedures defined into the quality management process.

From a safety management point of view, each time a modification/evolution is proposed, the safety manager should review/assess the proposal in order to

- identify which lifecycle phases are impacted,
- which kind of safety/hazard analysis should be updated in order to assess the safety criticality of the changes (in simple cases one dedicated safety studied can be enough to address the modification),
- which lifecycle phase review should be repeated to finally approve the evolution/modification,
- which documentation is impacted and should be updated,
- trace the actions into the hazard log.

The above results / actions should be included in a dedicated report as a result of the decisions taken by the Change Control Board in charge of the evolution/modification.

This should be referenced in the Safety Case as justification and rationale for the safety management of the evolution/modification to record that the Evolution/Modification is acceptable from the view of the safety management.

5.2.3.9 Safety Verification and Validation

This subclause gives guidance on EN 50129:2003, 5.3.9.

In addition to the addressed activities and their organizational requirement, also in case of any modification of the system/sub-system/equipment, according to EN 50129:2003, Figure 6 and Table E.9, V&V activities are further considered as far as the “left-side branch” activity in the V-Life-cycle is concerned. These activities should be conducted either within the organization or with intervention of external assessors The Safety Authority role in EN 50129 is confirmed in case of final Verification and Validation.

Validation implies knowledge of the system which means that adequate check of the requirements/prerequisites/assumptions, formula used, etc. are necessary for the validation. This means also activities on the left side while the resulting validation takes place on the right side, till a real application is used and the resulting behaviour for different aspects/properties is known.

The combination of “Safety evaluation on Verification” on the top-down branch of the lifecycle in addition to the “safety validation” on the bottom-up branch of the lifecycle should ensure completeness for the final “validation” evidence.

5.2.3.9.1 Safety Verification

Safety Verification has the purpose to demonstrate by means of analysis and test that the design solution is complete according to the required safety integrity level. This demonstration is performed at each phase of the V-lifecycle and is achieved by

- analysis performed to identify the correctness and the completeness of the specifications and design solutions. The identified safety requirements should be traced to design documents. This activity is mainly performed during the top-down branch of the V-lifecycle. Analysis cover also manufacturing specifications, installation design, operational rules and maintenance topics. Traceability of safety requirements should therefore be extended to manufacturing / acceptance procedures, installation and configuration procedures, operational rules and maintenance plans / procedures,

- testing / simulation performed during the bottom-up branch of the V-lifecycle to verify the correctness of the design implementation according to design specifications, compliance of manufactured products to the specification, compliance of the installation to the specification. These methods also complement safety studies in the top-down branch of the lifecycle, whenever analytical methods do not allow to analyse all possible failure modes.

These activities are performed in different steps according to what defined in the Safety Plan or V&V Plan and provide information to be registered in the Hazard Log.

Every safety requirements that cannot be verified within the scope of the reference project, has to be exported as safety-related application conditions.

5.2.3.9.2 Safety Validation

This section reports the results of the safety validation activities carried out during the bottom-up branch of the V-lifecycle as planned in the Safety Plan. A safety validation activity consists in safety validation tests and on the inspection that all the activities of the lifecycle have been successfully performed.

The extent of the safety validation tests can be defined taking into consideration the level of evidences produced by the tests executed during the previous verification activities. In this case, as for all the other phases, the safety independent team has to perform an assessment on the process and results of those tests. If the test activities are not carried out directly by the validation team, then the validation activity should include the review of all test specification/procedures and results.

The previous V&V safety validation activities have to be reported either in the Safety Case or/and in a dedicated overall Safety Validation Report, to which the Safety Case refers.

These activities are part of the Safety Management Report.

In complement to the V&V related activities, this final report also has to present evidence on the points related to the above V&V activities and to the following related activities:

- evidence of closure of all safety Requirements (in Hazard Log, in a specific document or in this final report) by means of tests, analysis, validation or accepted exported constraints. All non-closed points should be assessed against existing mitigation or specific exported operation constraints;

- report on Hazard Log (if not completed above), with, assessment on open points;

- report on Change Control board activities, with safety team participation, and whenever applicable, evaluation of open points (if not completed in the Hazard Log or in a dedicated section);

- checking of compliance with all applicable standards;

- Safety evaluation on V&V processes. For instance, for data Preparation & Validation and Test & Commissioning;

- evaluation on tools used in the V&V process;

- evaluation on change management process, and in particular concerning regression tests and strategy for non-completely validated intermediate versions.

5.2.3.10 Safety justification

This section should recap the conditions allowing the system acceptance by the Safety Authority in order to obtain the handover of the system. The list of conditions other than compliance to CENELEC standards should be provided like compliance to other regulations if any, evaluation and management of exported of safety related application conditions.

The global safety justification is provided by the entire Safety Case jointly with documents referred to.

However it can be stated here that the points related to the final acceptance, as agreed with the Safety Authority are described in this section, and are related to

- the current Safety Case completeness or status,
- the strict compliance of the process with the applicable standards, company manuals and Customer requirements,
- the assessment and/or the certification by an ISA or a Notified Body,
- the rigorous follow-up and internal examination on the following topics: Hazard Log, Safety Audits, Quality Audits, Safety reviews, safety assessment of Change Control Board, and Verification and Validation.

In particular, the assessment on restrictions and existing mitigation on remaining open points, if any, also assessed by the ISA (or other competent Authority) stated on previous sections and recalled in the conclusion section of this document are essential for safety justification on the operation of the system/subsystem/equipment accordingly to the currently delivered Safety Case.

5.2.3.11 System/Sub-system/Equipment handover

This section in the Safety Management Report should describe (if applicable)

- the system/subsystem/equipment has been developed in the context of a contract defining a specific Acceptance/Approval process with a specific customer, or
- the system/subsystem/equipment has been developed as Generic Product/Application for which an Acceptance/Approval should be defined.

In the first case, as an example, this section could be developed as follows, referencing the relevant documents.

> This section describes the process agreed between the Supplier, Railway Authority and the Safety Authority [4] to obtain the safety approval and safety acceptance of the system/subsystem/equipment as specified in EN 50129:2003, 5.5.
>
> The main steps should be
>
> - provision of the “Conditions for Safety Acceptance”: this activity consists in the issue of the Safety Case and all related documentation by the Supplier organisation. A list of the applicable documents associated to the Safety Case should be reported in the Safety Case itself,
> - independent Safety Assessment: this activity consists in the evaluation of the adequacy of the “Conditions for Safety Acceptance” by an independent organisation (possibly agreed between customer and supplier). The activity will issue a “Safety Assessment Report”. A reference to ISA Reports and conclusions (when available prior to the issue of the Safety Case) should be reported in the Safety Case itself. If ISA results will not be referenced by the Safety Case but will be covered in a subsequent phase, this should be clearly stated,
> - Safety Approval: this activity consists in the approval of the system/subsystem/equipment by the Safety Authority based on the results of the “Conditions for Safety Acceptance” and of the “Safety Assessment Report”. The activity will issue a “Safety Approval certificate”. A reference to the process defined in the contract should be provided,

[4] Involved Authorities and parties are subject of National and European Regulations.

- Safety Acceptance: this activity consists in the acceptance of the system/subsystem/equipment by the Railway Authority based on the results of the “Safety Approval”,
- a reference to the process defined in the contract should be provided.

In the second case, the Safety Case should propose a process between the Supplier and the Railway Authority in order to obtain the safety approval and safety acceptance.

In case of migration with an overlap between new and old system / Subsystem / Equipment, complementary processes have to be assessed which correspond to intermediate phases described in 6.2.

5.2.3.12 Operation and maintenance

This section in the Safety Management Report should describe the extent on which the Safety Management process has addressed the ”Operation and Maintenance” phases, i.e. which kind of Hazard and Operability studies have been performed and with which coverage.

As an example it should be stated providing related references, if the Safety Management process and related Safety Case have identified the ”Operation and Maintenance” rules to be applied in nominal and/or degraded modes of

- the system/subsystem/equipment,
- the behaviour of operators (drivers, train dispatchers, etc.),
- the behaviour of maintenance staff;

Based on the extent of the above analysis, this section should describe which ”Operation and Maintenance” analysis are covered by this Safety Case and what should be covered by an additional Safety Case. As an example, it should be stated if

- the performed analysis and therefore this Safety Case fully covers and defines the rules for a safe ”Operation and Maintenance” of the system/subsystem/equipment,
- the Safety Case does not cover Hazard and Operability safety studies, therefore a dedicated Safety Case should be provided,
- the Safety Case covers only partially Hazard and Operability safety studies, therefore it is of the responsibility of the Railway Authority to complete the process and define the rules for a safe ”Operation and Maintenance” of the system/subsystem/equipment.

As a basis for the Hazard and Operability safety studies, it should be referenced EN 50129:2003, Table E.10 of the standard, including also possible behaviours of the maintenance staff.

The following lists of documents should be referred

- list of User Guides/Manuals,
- list of Operation and Maintenance Manuals/Procedures,
- list of Training courses led by the supplier to Railway Authority personnel.

5.2.3.13 Decommissioning and Disposal

In application of the life cycle a system should remain safe from the first phase until the last phase “Decommissioning and Disposal”. This section should report the precautions to which Decommissioning and Disposal procedures should take care of.

EXAMPLES for Decommissioning (technical safety precautions and procedures):

- switch-off of the system in a safe state;
- disconnection of the links with the environment (I/O, Transmission, power supplies, etc.);
- if applicable, migration phases for introduction of replacement systems;
- etc.

EXAMPLES for Disposal:

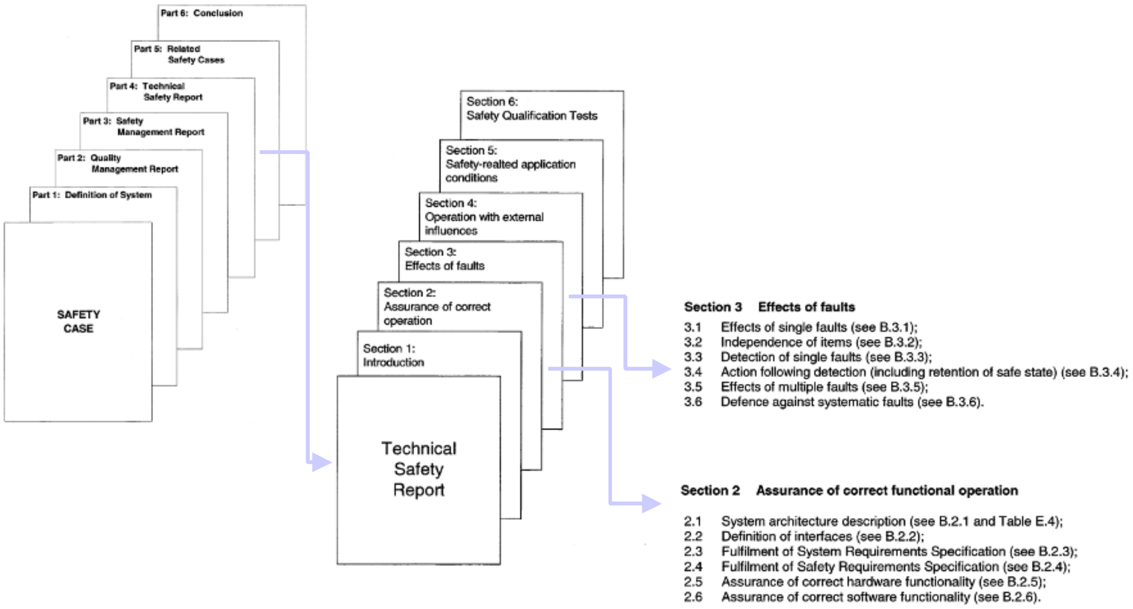
- precautions to avoid electric shocks;
- storage precautions for flammable / toxic materials (reference to national laws and EC directives);
- etc.

5.2.4 Technical Safety Report structure

According to EN 50129:2003, 5.4, the Introduction (i.e. Section 1) of the Safety Case Part 4 (i.e. Technical Safety Report) should give a summary of the safety principles, the extent of safety measures and the list of reference standards relevant to the considered system, subsystem, equipment.

The adopted s7afety principles should be described as follows (see also Figure 13):

- Section 2 of the TSR (see EN 50129:2003, 5.4) requires to demonstrate the correct operation under fault-free normal conditions and to describe how safety requirements are fulfilled;
- Section 3 of the TSR (see EN 50129:2003, 5.4) requires demonstrating how safety requirements continue to be met in the event of random hardware faults.


Part 6: Conclusion
Part 5: Related Safety Cases
Part 4: Technical Safety Report
Part 3: Safety Management Report
Part 2: Quality Management Report
Part 1: Definition of System
SAFETY CASE
Section 6: Safety Qualification Tests
Section 5: Safety-realted application conditions
Section 4: Operation with external influences
Section 3: Effects of faults
Section 2: Assurance of correct operation
Section 1: Introduction
Technical Safety Report

Section 3 Effects of faults

3.1 Effects of single faults (see B.3.1);
3.2 Independence of items (see B.3.2);
3.3 Detection of single faults (see B.3.3);
3.4 Action following detection (including retention of safe state) (see B.3.4);
3.5 Effects of multiple faults (see B.3.5);
3.6 Defence against systematic faults (see B.3.6).

Section 2 Assurance of correct functional operation

2.1 System architecture description (see B.2.1 and Table E.4);
2.2 Definition of interfaces (see B.2.2);
2.3 Fulfilment of System Requirements Specification (see B.2.3);
2.4 Fulfilment of Safety Requirements Specification (see B.2.4);
2.5 Assurance of correct hardware functionality (see B.2.5);
2.6 Assurance of correct software functionality (see B.2.6).

Figure 13 – Structure of the Technical Safety Report

Nevertheless, for signalling functions it can in practice be difficult to separate functions under normal conditions and conditions in case of failure. Since the two behaviours often can be part of the same function, a separated description in different sections can render understanding and evaluation difficult, even if it is possible to separate them.

It could be convenient to introduce the safety principle associated to each function where its normal behaviour is also specified (e.g. Section 2 of the TSR in EN 50129:2003, 5.4).

This guidance provides example of functional and safety principles described in Section 2 of the TSR (EN 50129:2003, 5.4) where also demonstration of their integrity fulfilment is provided, while Section 3 of the TSR (EN 50129:2003, 5.4) will be focussed on the demonstration by analysis of the fulfilment of safety integrity requirements associated to all possible failure and degraded modes, relevant to each considered function, including the existing or expected mitigations (ref. to Section 5 of the TSR in EN 50129:2003, 5.4, namely Safety Related Application Conditions).

In particular Section 2 of the TSR (EN 50129:2003, 5.4) should detail the architecture description given in 6.2.1 and describe the safety principles at different level of abstraction depending on the level of complexity of the project, i.e. system, subsystem, equipment.

Considering that the extent of the safety measures is depending on the application and on the SIL to be reached, a presentation of the adopted criteria and assumptions, according to the actual implementation, should be given in Section 1 of the TSR (EN 50129:2003, 5.4).

5.2.4.1 Introduction (EN 50129:2003, 5.4, Section 1)

This section complements the Introduction part of the Safety Case (refer to 5.2.1).

The list of standards concerning safety, used for the system / sub-system / equipment development, should be given in the TSR. In certain cases, it is impossible or difficult to quote standards: case of an old equipment developed when this kind of standards did not exist, or developed in accordance with standards out-of-date today. In these cases, explain the lack of standards or quote former local technical standards (see also 6.2). If possible, establish a correspondence with current standards, or refer to applicable Code of Practice, according to the Definition by the European Railway Agency.

5.2.4.2 Assurance of Correct Functional Operation (EN 50129:2003, 5.4, Section 2)

5.2.4.2.1 System Architecture Description

The following points should be described with a synthesis and/or providing reference to the available documentation:

- description of the system / sub-system / equipment as evolution of a previous version, if needed;
- presentation and analyses of functions committing safety (or new functions, if needed) with their SIL classification;
- degraded modes operation definitions and management as specified in relevant design documents;
- presentation of the affected architecture;
- presentation of safety principles used (if possible face to face with different presented functions (previous item);
- presentation of re-used functions with their safety justification;
- presentation of the safety level reached in line with standards and criteria used;
- first presentation of the conditions of use and condition of operation guaranteeing the considered safety level.

It is important to introduce the technical safety principles on which the project is based. Block-diagrams and schemes can usefully be used to clarify the above points.

Subclauses 5.2.4.2.1.1 to 5.2.4.2.1.3 give examples of technical safety principles to be described or referenced through available documentation.

5.2.4.2.1.1 Examples at system level

At system level some examples could be

- interlocking system,
- ATP / ATC system for interoperable high speed lines,
- ATP / ATC system for national lines.

At this level the basic signalling safety principles should be described and provide reference to their specification and related methodology (structured approach, formal methods. etc.). Whenever transitions between different systems are allowed, justifications of the principles that help with avoidance of impact on safety should be explained / referenced.

In order to ensure the correctness and completeness of the safety principles, evidence of their validation should be provided and referenced. This can include

- validation by simulation of the signalling model,
- formal proof based on model checking / theorem proving of the safety properties.

If the signalling principles have been already used in similar existing system, they could be considered as “proven in use”, providing the references.

Examples for an Interlocking system

Safe Signalling rules are often defined by national railways through general “signalling principles”. They can include the function of setting a route for a train.

This function can be based on a sequence of actions:

- request by an operator for a specific route;
- check by the system for the availability of the needed resources and in case of success their locking;
- check by the system for the absence of conflicting routes;
- in case of success, activation of the permissive signals to trains, otherwise release of the resources.

Examples for an ATP / ATC system for interoperable high speed lines.

Typical ATP / ATC uses signalling principles based on the concept of “Movement Authority”:

- a train requests the authorisation to movement providing its identifier;
- the trackside checks for the availability of the needed resources and absence of conflicts. In case of success it provides their locking;
- the trackside provides a movement authority to the train in term of distance and speed by means of continuous and / or discontinuous signalling;
- the train supervise its movement based on the received information, its current speed and the model of its braking capability.

5.2.4.2.1.2 Examples at subsystem level

Based on the safe signalling principles required at system level, at subsystem level the safety principles adopted for the design should be described and justified.

Some examples:

Principle of the closed loop:

If one safety related information is sent from a source to a user, the source expect to have a coherent feed-back, otherwise it apply a fall-back policy.

Control / command of switching point: the interlocking equipment controls the switch machine according to the intended route. The same equipment checks for a position control of the switch machine coherent with the control before to authorise final permissive actions.

Management of the status of a track circuit: the status of a track circuit “free / occupied” can be managed by means of an equipment that injects a signal at one end of the track circuit. The track circuit is considered free if and only if the same equipment is able to receive from the other end of the track circuit a signal with a pre-defined relationship with the injected signal.

Principle of dynamic signals:

A permissive state of one information should be associated to a signal with dynamic characteristics.

Movement Authority sent to a train by means of continuous signalling: a train recognises a movement authority as valid only if the used signal is dynamic.

ERTMS Level 2 uses the “Euroradio” protocol where each new message contains a different sequence number. If the train does not receive an updated information, the old information will expire applying a safe reaction.

ERTMS Level 1 uses a spot transmission by means of balises. Since the transmission is “open loop” and the telegrams do not contain any dynamic information, the information could be not receivable by trains. This lack can be mitigated using the concept of “linking“ between consecutive balises on the track. In case of missed link, the train apply a safe reaction.

National ATP subsystems uses a pre-defined set of signals, where each signal or transition between two signals is associated to a signalling condition. Used signals are dynamic signals, and the case of absence of a signal is associated to a restrictive state.

5.2.4.2.1.3 Examples at Equipment / Product Level

Based on the design principles required at subsystem level, at product level the safety principles adopted for the design and implementation should be described and justified.

The basic safety principles are based on the definition provided in EN 50129:2003, B.3.1:

— inherent fail-safety (see item a) below);

— composite fail-safety (see item b) below);

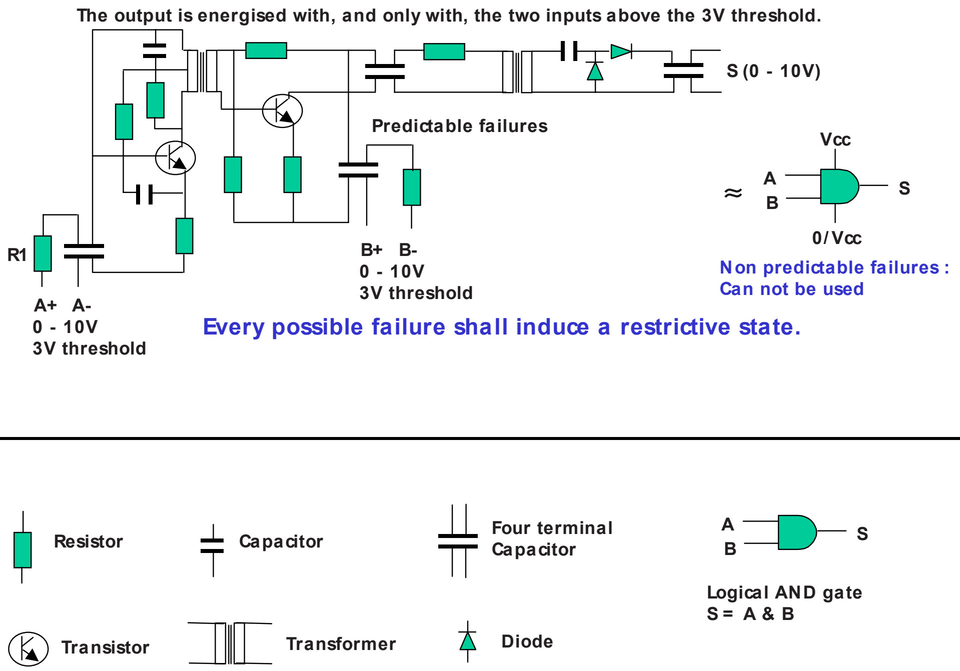
— reactive fail-safety (see item c) below).

a) Example of inherent fail-safety (see Figure 14)

AND function

For a simple AND function, its implementation by means of integrated logical ports can lead to unpredictable failure modes. Therefore it can not be used in a safe design.

By using well known elementary functions and components, it is possible to implement inherent fail safe composite functions, where every possible failure induces a restrictive state.



An inherent fail-safety proof shall be based on particular steps. For example:

•An FMEA is performed against the circuit diagram and all possible failures are assessed as not inducing wrong side failure by activating a permissive output state.

•This is not possible with a single gate component, where all failure modes are possible.

•Inherent fail safety imposes the use of specific components as four terminal resistors and capacitors.

Figure 14 – Example of inherent fail-safety

b) Case of the composite fail-safety

Typical examples of implementation adopting the “composite fail-safety” criteria are the platforms using redundancy with an NooM voting criteria.

As an example, and referring to Clause 5, the safety principles for this type of architecture will be described among the following:

- prevention of Hardware systematic failures as
  - Built-in-Tests,
  - partial hardware diversification,
  - encoded protection,
  - diversified memory allocation,
  - digital hardware diversification,
  - analogue parts enhanced with level detection,
  - inherent fail-safe circuits,
  - partial FPGA diversification and use of dynamic signals;
- prevention of Software systematic failures (according to EN 50128) as
  - software development process,
  - compiler diversification,
  - Target Modular Tests,
  - compilers and tools validation;
- prevention of external and internal perturbations as
  - isolation barriers,
  - de-synchronisation by compilers,
  - natural de-synchronisation,
  - time execution and coded diversified doubled software modules,
  - channels carrying complementary information;
- prevention of Hardware single and dormant failures as
  - Built-in-Tests,
  - voting,
  - jamming,
  - code (n bits) protection,
  - inherent fail-safe design,
  - design criteria of all single failures detected and probabilistic wrong side failure calculation for all identified dormant failures.

c) Case of the reactive fail-safety

In this case, most of previous mitigation may apply and will be also described.

However, specific points are to be taken into account and described, whenever applicable:

- single processor with coding techniques ensuring protection against HW systematic and random failures;
- auxiliary processor ensuring coded data checking;
- safety guaranteed reaction times;
- re-reading and specific techniques for output interfaces;
- watch-dog techniques;
- others.

5.2.4.2.2 Definition of Interfaces (see also EN 50129:2003, B.2.2)

Because safety relies also on external interfaces, a particular care has to be carried out on a clear definition of the external interfaces.

Although EN 50129:2003, B.2.2.2 deals with functional and physical requirements of the System interfaces, the designer should focus on the safety principles, either of internal or external interfaces, on which their safe state is ensured.

For example:

- presence of energy over a pre-defined threshold;
- dynamic characteristics of the signal;
- double condition with diversity (contact normally open and normally closed associated to each input).

These requirements represent the basis for the application conditions to be exported from “Generic Products” to “Generic Applications” and “Specific Applications”.

Some examples:

- For single Boolean inputs and outputs it should be specified if there is one of the two possible states (TRUE or FALSE) that can be associated to a conservative safe state.
- For serial data (message transmission) it should be specified if there is any assumption on the effect of sending corrupted messages that can be detectable by the user or in non receiving expected information.
- For analogue data and pulses streams the functional impact on accuracy and its effects should be specified if no data is available.

5.2.4.2.3 Fulfilment of System Requirements Specification (see also EN 50129:2003, B.2.3)

The requirements specified in the SRS should be classified by means of attributes on which the demonstration strategy should be based. This section should summarise the identified classes and the chosen method for demonstration strategy.

Fulfilment of System Requirements Specification is demonstrated by means of Verification and Validation activities. Reference to Verification Reports and related results should be reported in this section, with an evaluation/justification in case of open points.

Functional requirements should always be demonstrated by specification and execution of functional tests. The criteria on which the test cases are chosen should be justified (e.g. equivalence classes). Completeness of closure should be indicated by reference to a traceability document.

Performance requirements can be demonstrated by combination of test results and calculation. A strategy should be defined to demonstrate that the requirements continue to be fulfilled not only in the lab but also under operational conditions in the context of a field trial for example.

Reference to Validation / Tests Reports and related results should be reported in this section, with an evaluation/justification in case of open points.

5.2.4.2.4 Fulfilment of Safety Requirements Specification (see also EN 50129:2003, B.2.4)

Safety requirements can be demonstrated by combination of analysis and tests.

The demonstration of the fulfilment of Safety Requirements should address two attributes defined during the hazard analysis on the top-down branch of the V-lifecycle:

- Functional Safety, based on the expected behaviour of the system/subsystem/equipment under normal conditions and when deviated events are applied, including the reaction time required for it;
- Safety Integrity, based on
  - the adoption of qualitative measures to reduce the effect of systematic and random errors, and
  - the quantitative evaluation of the hazard rate associated to the hazardous events for estimation of residual risk.

Functional Safety should be demonstrated providing evidence of the corresponding requirements in the design solution and of the related test cases and test reports. Test cases should also specify the expected reaction time.

The safety test specification should be based on a systematic approach. For example it could be based on the failure analysed during HAZOP and FMECA studies.

Safety Integrity Requirements can be demonstrated by means of analysis and calculation, combining the failure rates of components, time between events, and the coverage of the safety measures.

This subsection of the Technical Safety Report should provide a complete justification (if not done in the Safety Management Report) by claiming the following:

- reference (to the overall safety validation report) or presentation of the closure of all safety requirements by verification, analysis or validation (including SW verification, HW verification, requirement testing, type testing, etc.). This is stated in the Safety Verification and Validation subsection of the Safety Management Report. Also complete reference to the "horizontal" traceability (indication of closure for every safety requirement, by verification, tests, validation, critical code review or specific assessment) has to be referred to, or reported in an annex to the Safety Case;
- additional reference or presentation of similar systems can be made to demonstrate that safety is not degraded.

Safety requirements from the upper level system have to be stated as fulfilled with the related justification.

5.2.4.3 Effect of Faults (EN 50129:2003, 5.4, Section 3)

This section should describe the details of the safety analysis to ensure that no single fault would lead to any hazardous condition and to identify possible multiple faults. This is a basis for further quantitative safety analysis.

Hereafter some examples of safety principles used depending on the requirements are presented. The aim is to provide some guidance on the type of information. For complete description specific and exhaustive documents should be referenced.

EN 50129:2003, Clause B.3 defines mandatory subsections in the Safety Case:

- effects of single faults (EN 50129:2003, B.3.1);
- independence of items (EN 50129:2003, B.3.2), related to internal and external, functional and physical influences;
- detection of single faults (EN 50129:2003, B.3.3);
- action following detection (EN 50129:2003, B.3.4);
- effects of multiple faults (EN 50129:2003, B.3.5);
- defence against systematic faults (EN 50129:2003, B.3.6).

In an efficient integrated approach with a careful selection of methods as argumented in the Safety Management Report section, the content of these sections can be based on the output created by the safety analyses methods.

For EN 50129:2003, B.3.1 “Effect of single faults”, the results of FMEAs or HAZOP are completely sufficient. The FMEA also identifies the failures to be detected. The detection means should refer technical safety principles collected and described in the Section 2 of the TSR “Assurance of Correct Functional Operation” (EN 50129:2003, 5.4).

If FTA or Markov models are used, then during application of any of these methods the questions related to EN 50129:2003, B.3.2 “Independence of items”, EN 50129:2003, B.3.3 “Detection of single faults” and EN 50129:2003, B.3.4 “Action following detection” have to be answered. This usually includes a CCF analysis.

The purpose of the common cause failure analysis is to identify any case in which two or more events could occur as the result of a common event or causative mechanism. If the probability of a common cause is significantly greater than the probability of the two or more events occurring independently, then the common cause could be an important risk contributor. This task is very important e.g. for the proper handling of AND gates in fault trees, where independence is assumed.

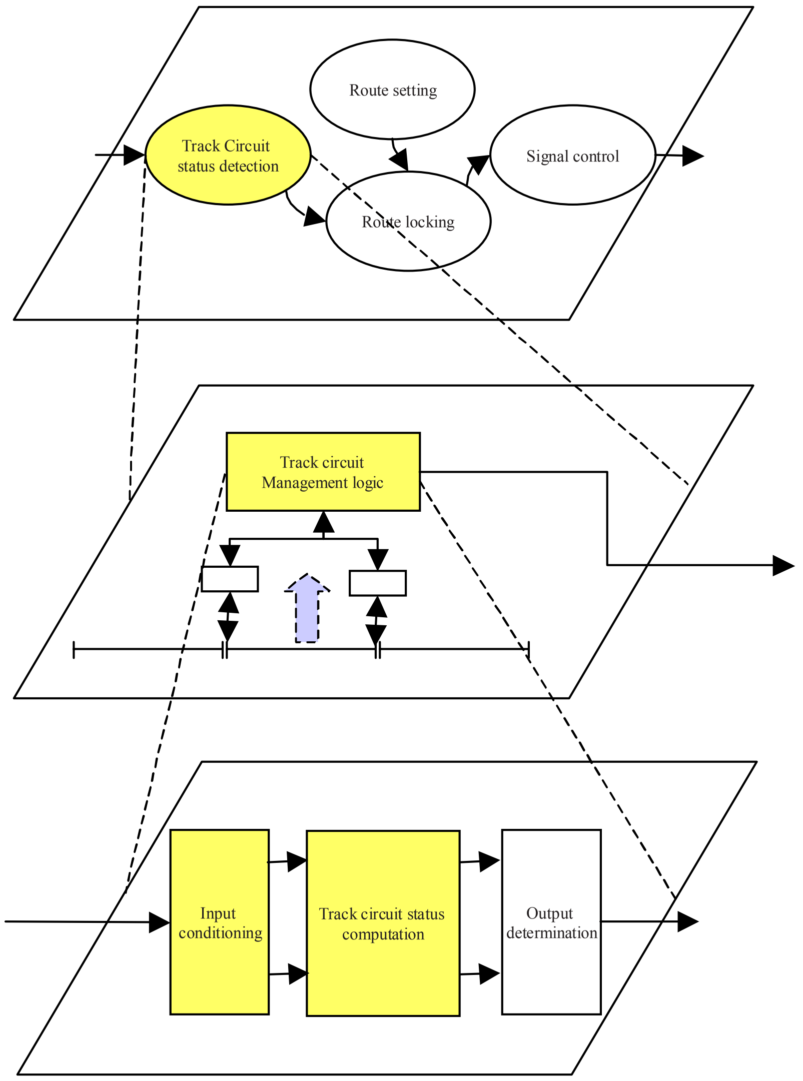
The complete FTA or Markov model is described in EN 50129:2003, B.3.5 “Effects of multiple faults”.

All the safety analysis should be based on a meaningful model of the system description at the different hierarchical levels of the development phases and on the coherence of the difference safety analysis.

Figure 15 provides an example of system description at different hierarchical levels showing the different levels of safety analysis and possible relationships to ensure coherence and completeness.

NOTE If applicable, an issue can be completely managed in one section and referred to in another subclause.

In Figure 15 on the left side it is showed how the causes of hazardous conditions identified at one level of abstraction by FMECA, can usually represent effects for deviations for FMECA at lower levels of abstractions.


Track Circuit status detection
Route setting
Signal control
Route locking
Track circuit Management logic
Input conditioning
Track circuit status computation
Output determination

Function	Falure Mode		Effect/Hazard	Measures	
Track circui status detection	[wrong] undue free status detected		undue route locking	Safety principle #1 (dynamic and diversified signal for TC)	

Function	Falure Mode		Effect/Hazard	Measures	
Track circuit management logic	[wrong] undue free status detected		undue route locking	Safety principle #2 (cyclic elaboration and association of occupied status as safe state	

Function	Falure Mode		Effect/Hazard	Measures	
Input conditioning	[wrong] status stucked at ON (free TC)		undue free status detected	Safety principles #3 (inherent fail-safe input conditioning)	
Track Circuit status computation	[wrong] undue free status computation		undue free status detected	Safety principle #4 (composite fail-safe for track circuit status computtaion)	

Figure 15 – Example for Relation between Design Functional Breakdown

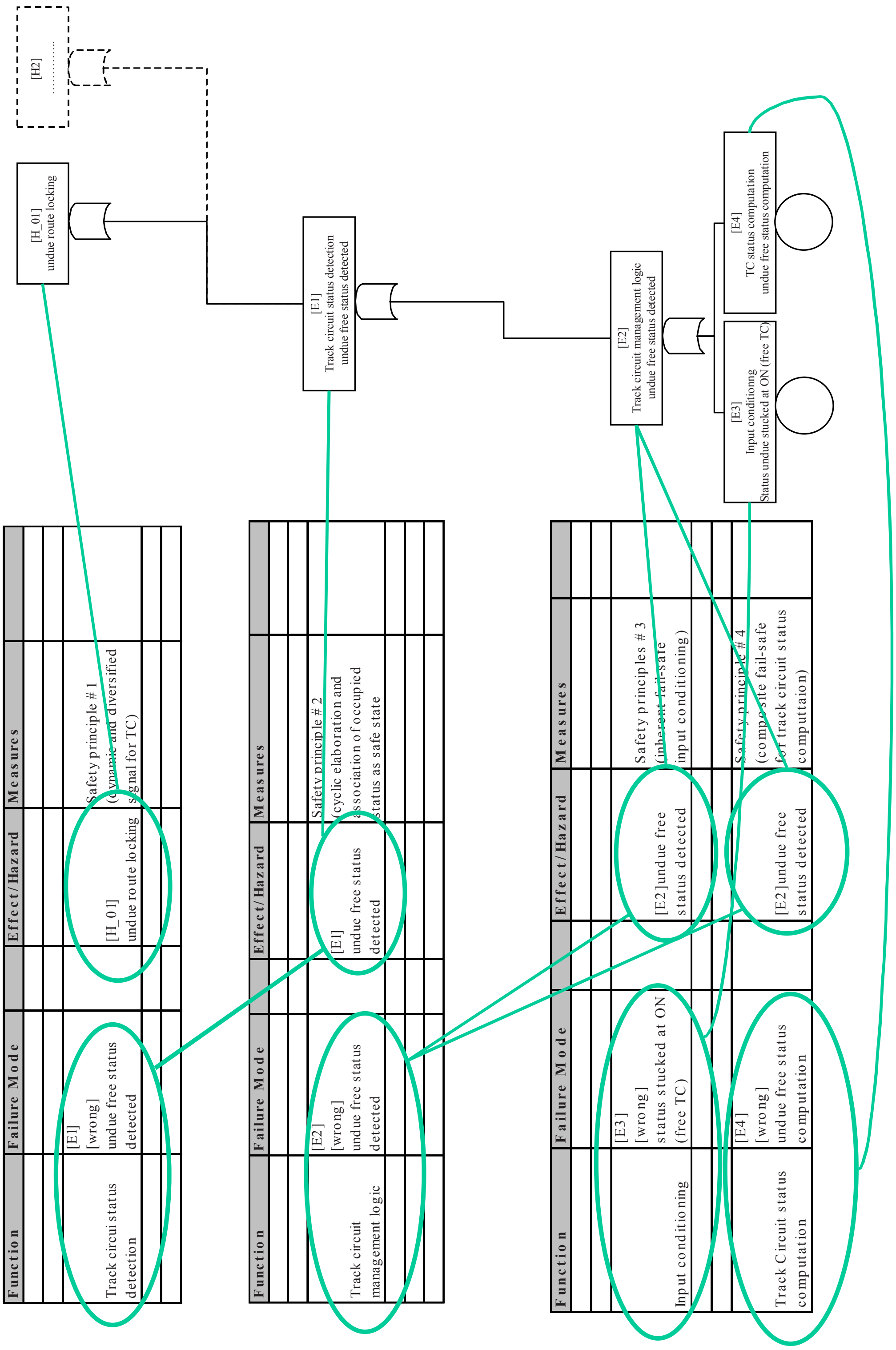

[H_01]
undue route locking
[H2]
…………
[E1]
Track circuit status detection
undue free status detected
[E2]
Track circuit management logic
undue free status detected
[E3]
Input conditionng
Status undue stucked at ON (free TC)
[E4]
TC status computation
undue free status computation
Function
Failure Mode
Effect/Hazard
Measures
Track circui status detection
[E1]
[wrong]
undue free status detected
[H_01]
undue route locking
Safety principle # 1
(dynamic and diversified signal for TC)
Track circuit management logic
[E2]
[wrong]
undue free status detected
[E1]
undue free status detected
Safety principle # 2
(cyclic elaboration and association of occupied status as safe state
Input conditioning
[E3]
[wrong]
status stucked at ON
(free TC)
[E2]undue free status detected
Safety principles # 3
(inherent fail-safe input conditioning)
Track Circuit status computation
[E4]
[wrong]
undue free status computation
[E2]undue free status detected
Safety principle # 4
(composite fail-safe for track circuit status computtaion)

Figure 16 – Example of Relation breakdown from FMEA to FTA

A meaningful definition and proper labelling of the events (deviation, causes and effects) represents a database of reference hazardous conditions to be used at the following levels avoiding the generation of new events not useful, saving time and resources.

Furthermore labels can allow traceability to investigate the propagation of the effects at different levels.

On the right side of Figure 16 it is proposed an example of top-down analysis by Fault Tree Analysis technique. This analysis complements the bottom-up analysis, allowing to identifying hazardous conditions generated by combination of multiple causes and / or common cause failures. Usually most of the events (Top events, Intermediate events, Basic events) are the ones already identified in the bottom-up analysis, allowing a crosschecking for completeness and correct propagation and traceability from a qualitative point of view.

The identified model for the Fault Tree Analysis can then be used also for quantitative evaluation of the Hazardous Failure Rates, as soon data for the basic events are available.

While bottom-up techniques are more systematic, it is very important that Fault Tree Analysis is performed by skilled people able to properly create a model taking into account all the parameters that can influence the final result especially when using combinatorial AND gates (selection of rates instead of probabilities, initiating and dormant events, repairing/inspection time, reference life-time for the computation).

Depending on the level of details of the latest level of FMECA, specific basic events could be further analyzed by means of specific technique (Markov models for combination of multiple events, component failure tests for inherent fail-safe circuits).

5.2.4.4 Operation with external influences (EN 50129:2003, 5.4, Section 4)

EN 50129:2003, Clause B.4, provides complete information on this topic.

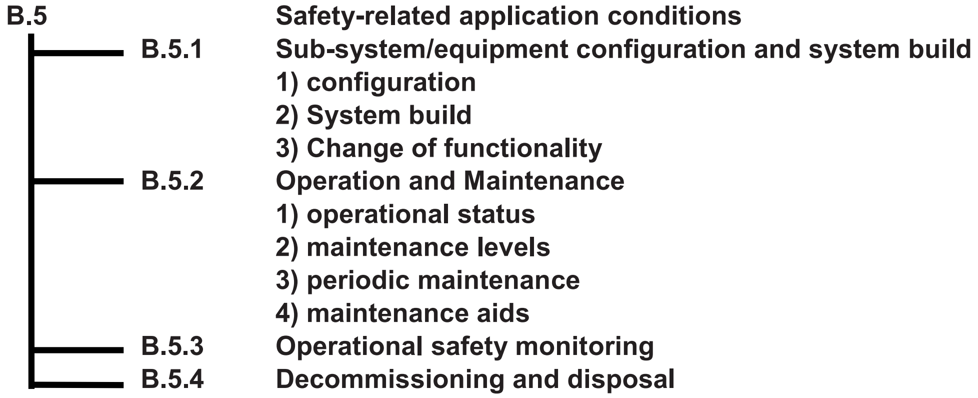
For all the classes of external influences defined in the standard, it should be referenced the documentation providing the related evidences. This should be taken into account during the safety analysis according to the criteria given in Clause 4.

5.2.4.5 Safety related application conditions (EN 50129:2003, 5.4, Section 5)

It is considered that EN 50129:2003, Clause B.5, is fully developed and provides suitable information, except for system / sub-system / equipment exported constraints.

SRACs are generated by safety analysis at each level of the project whenever a related Safety Case has been identified or not.

A classification following the classes recommended by EN 50129:2003 is useful for final users to ensure that each stakeholder will address the ones of its own responsibility (see Figure 17).



B.5 Safety-related application conditions

- B.5.1 Sub-system/equipment configuration and system build
  1) configuration
  2) System build
  3) Change of functionality
- B.5.2 Operation and Maintenance
  1) operational status
  2) maintenance levels
  3) periodic maintenance
  4) maintenance aids
- B.5.3 Operational safety monitoring
- B.5.4 Decommissioning and disposal

Figure 17 – SRAC classification

According to the structure shown in Figure 17 above, the exported/imported SRACs should be classified and traced, so that it can easier be monitored in the verification process.

When exporting SRACs from one lower level to an upper one, part of the inherited SRACs can be closed with evidences addressed by new hierarchical level, while new SRACs can be generated by the additional safety analysis. So far these inherited SRACs are not closed and the new ones generated constitutes the new set of SRACs applicable to the identified next level.

The process is re-iterated till the latest level of Safety Case depending on the scope of the project. The latest set of SRACs represents the last result to be exported to the final user of the project.

The management of the exporting process in general could not be managed only inside the Safety case itself, but it should be controlled along all the lifecycle inside the Hazard Log (reporting inside the Safety Case only the net result of open exported SRACs).

A special mention is needed when a Generic Product or a Generic Application Safety Case is concerned.

It is crucial that SRAC´s are explicitly listed in a Generic Product or a Generic Application Safety Case, so that they can be exported and taken into account by the specific application using the generic ones.

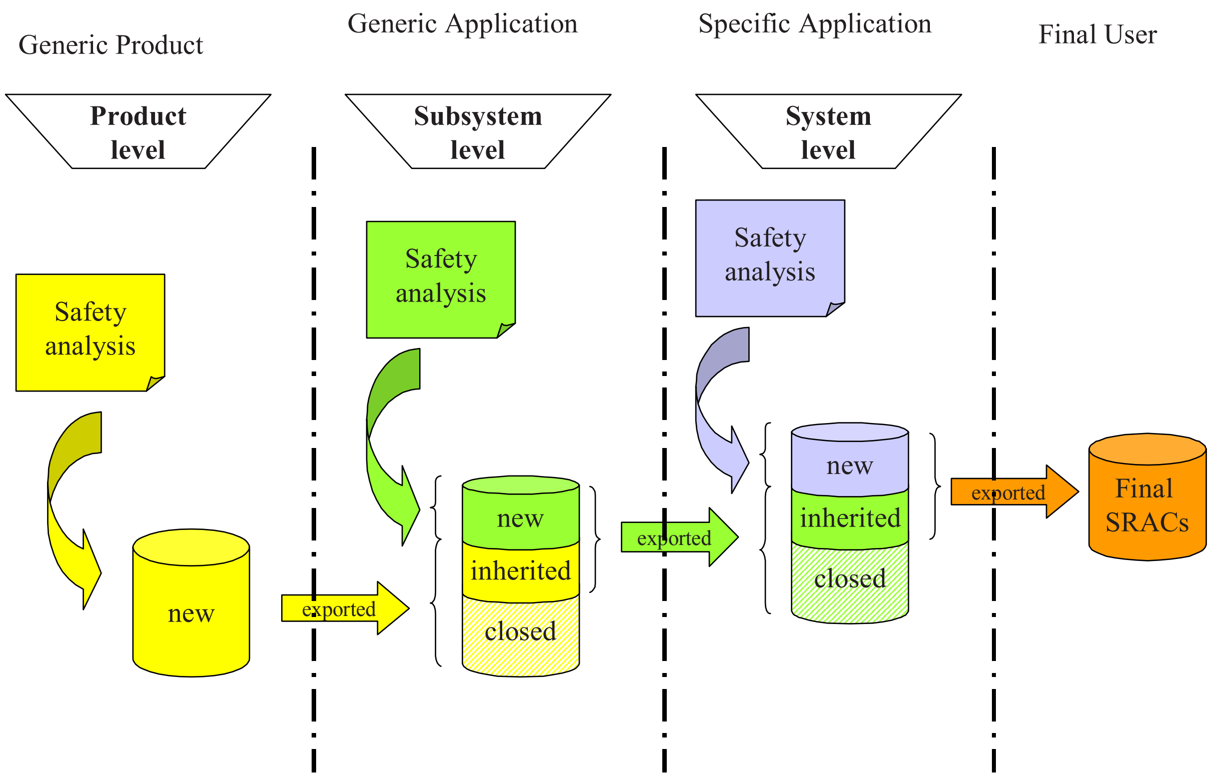


Figure 18 – Exported constraints and SRAC management

Exported constraints (see above Figure 18) have to be clearly identified in every lifecycle phase (system manufacturing / installation / configuration, operation, maintenance, etc.) according to what defined in the safety management process.

Every exported constraint will refer to the document/analysis, which issued it, and an assessment should be done on its criticality and related items.

Based on “Related Safety Case” section, this section should report also all exported constraints from lower level subsystems / products not closed at this level and that needs to be re-exported to higher level system.

Attention should be taken that only SRACs are exported which cannot be fulfilled in the respective Safety Case, and that no new safety requirements are generated having the form of SRACs.

The generating of SRACs has to be controlled always by the V&V process.

This section should not just specify separate SRACs notes to pop up without any source and any other location than in the safety cases. SRACs should be notified in User application documents or user manuals allowing actions being controlled from them, for every day usage or usage on demand. Some examples are

- application Notes for system/subsystem/equipment configuration,
- User/Operator manual for system/subsystem/equipment,
- maintenance manual for system/subsystem/equipment,
- etc.

Deviations from reference specification related to equipment / generic products not solved can be handled in "Product Notes". These documents should be verified according to what defined in the safety management process with a clear statement that all safety related exported conditions are properly addressed in these documents.

The SRACs section of the Safety Case should therefore just refer these documents without listing hundreds of detailed requirements.

5.2.4.6 Safety Qualification Tests (EN 50129:2003, 5.4, Section 6)

5.2.4.6.1 Basics

The purpose of the Safety Qualification Tests is to obtain a higher level of confidence in the system/subsystem/equipment. This means it should be demonstrated that the specified operational requirements can be fulfilled by the system/subsystem/equipment under real operating conditions.

The Safety Qualification Tests will not provide complete evidence that the safety requirements are satisfied, since e.g. a safety-reaction of the system/subsystem/equipment will only occur as a reaction to a fault condition. Consequently, it won't be possible within the Safety Qualification Tests to completely test all (Safety) Requirements with reasonable effort. These tests should take place within the proof of correct functional operation (EN 50129:2003, Clause B.2). Further, the Safety Qualification Tests are not meant to demonstrate that the specified system requirements are fully met. The validation phase will provide this evidence.

During the Safety Qualification Tests, safety should not depend on the testing object because the Safety Case has in most cases not yet been finished at this time, and further safety deficiencies might be revealed. Additionally, evidence is required that the testing object will have no unwanted impact on currently operational safety systems.

5.2.4.6.2 Test locations

The test location should be chosen such that as many specified operational requirements can be demonstrated as ever possible. Ideally, the safety qualification tests will be performed at the final first installation site.

5.2.4.6.3 Extent and procedures

Based on specifications from the supplier and prior experiences of the railway authority, railway authority and safety authority need to agree on the extent of the Safety Qualification Tests. For the duration of the safety qualification tests, the participants have to agree on periodical reports about the progress and results (conclusions; unexpected events) of the safety testing. In principle, the Safety Qualification Tests should be performed without any change in hardware or software during the test period. Of course, reference has to be made in the safety case for previous test and trial running with mention of the number of hours/kilometres, to malfunctions, operation with restrictions, etc.

Prior to starting the Safety Qualification Tests, the participants (railway authority, safety authority, supplier) should agree on a procedure for modification during the test period (depending on the extent of the modification).

5.2.5 Related Safety Cases structure

By reference to the general Safety Case structure when applicable, as defined in 5.2.1.2 mention is to be done, in an embedded structure, to lower level Safety Cases, for instance Generic Product SC, if the current Safety Case relies on these Safety Cases, their content should be referenced. The existence of Upper level Safety Cases, for instance (System) Specific/Generic Application SC, could be mentioned to provide an overview of the project structure, but usually its content should not be referenced.

Whenever the safety demonstration relies on other safety cases, the hierarchy of the related referenced safety cases should be provided in a top-down structure starting from the current safety case, like described as an example in 5.2.1.2.

Usually it should be not referenced safety cases at higher level than the current one, since the completion of safety demonstration is based on a V-cycle requiring providing evidences at lower levels before closing validation at an upper level.

For each referenced Safety Case, the following items should be provided:

- version of the safety case document and related system/subsystem/product configuration. This configuration should match with the configuration described in EN 50129:2003, 5.1, Part 1 “Definition of System” of the current safety case. In case of discrepancy, justification of the differences should be argumented;
- information about its approval status and possible restriction of use;
- safety related application conditions: it should be declared where it has been provided evidence of the management of the safety related application conditions exported by the referenced safety case;
- for proven in use system/subsystem/product for which a safety case is not available, it should be provided evidence of existing acceptance and evidence of the management of the risk evaluation and acceptance in using such a kind of system/subsystem/product.

In case of system/subsystem/product provided by other suppliers, the safety case content could be not fully accessible for intellectual property reasons. In that case the relevant information like interface description, SRAC´s, operational and environmental conditions should be given in separate documents.

In case of re-use of proven in use sub-systems/products without associated CENELEC Safety Case should be mentioned:

- existing Safety and validation documentation and a safety argumentation;
- existing return of experience and information from field.

Proven-in use arguments in general may be located in TSR and also as supplementing the safety qualification test section and conclusion.

In case of embedded Structure of Safety Cases (refer to Figure 9 and Figure 14), this section should present subsections stating the closure of all imported constraints.

5.2.6 Conclusions structure

This final section should contain the evaluation summary on the system / subsystem / product stating that

- the system is suitable for the intended use (test running, trial running or revenue service),
- the Quality Management Process is controlled and no quality issues are open,
- the Safety Management Process is controlled and all safety issues are closed or forwarded to the system’s SRACs,
- the requested safety target has been reached,
- the system`s SRACs are defined,
- the SRACs of the related SCs are closed or forwarded to the system’s SRACs.

5.2.7 Annexes possible contents

The annexes may include files or tables, which could be too long in the different subsections of the Safety Case (Open points assessment and their mitigation, exported constraints, detail of modifications since last Safety Case version, description of the performed V&V activities in case of main or secondary system / subsystem / product versions, etc.).

5.3 Recommendations regarding the fulfilment of the requirements of tables in EN 50129:2003, Annex E

This subclause gives guidance regarding the fulfilment of some of the requirements in tables of EN 50129:2003, Annex E. It lists the original tables in EN 50129:2003, Annex E, and highlight the requirement of the issue. In addition, recommendations regarding the evidence and possible outputs are given classified according to the possible SIL levels from SIL 1 to SIL 4 in order to tailor the effort in evidence depending on the required SIL level.

5.3.1 EN 50129:2003, Table E.1 – Safety planning and quality assurance activities

(Referred to in EN 50129:2003, 5.2 an 5.3.4)

Table 9 – Safety planning and quality assurance activities

Technique / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Checklists	R: checklist of activities and items to be produced Requirement: Completeness of Safety and Quality processes Evidence: Prepared Checklists, covering all Life Cycle Phases addressing all critical RAM, Safety and Organisational Aspects Output: Judgement of completeness of Checklists		R: checklist of activities and items to be produced Requirement: Completeness of Safety and Quality processes Evidence: Prepared Checklists, covering all Life Cycle Phases addressing all critical RAM, Safety and Organisational Aspects Output: Judgement of completeness of Checklists	
2. Audit of tasks	R Requirement: Safety and Quality Plans implemented Evidence: Appropriate documents against each checklist item Output: Audit Report and potential corrective actions		HR Requirement: Safety and Quality Plans implemented Evidence: Appropriate documents against each checklist item Output: Audit Report and potential corrective actions	
3. Inspection of issues of documentation	HR: documents agreed between railway/safety authority and industry Requirement: Distribution and Configuration Management of Documents referenced in the Safety and Quality Plan Evidence: Distribution List and Change History of each document Output: Quality Management Report and potential corrective actions, Documentation Plan		HR: all documents Requirement: Distribution and Configuration Management of Documents referenced in the Safety and Quality Plan Evidence: Distribution List and Change History of each document Output: Quality Management Report and potential corrective actions, Documentation Plan	
4. Review after change in the safety plan	HR Requirement: Peer Review of any updates to the plan Evidence: Record of Peer Review Output: Report, assessing the impact of every change on Safety Organisation and Activities			
5. Review of the safety plan after each safety life-cycle phase	HR Requirement: Compliance with safety activities in Life Cycle Phases Evidence: Record of Safety Audit in each Life Cycle Phase, Hazard Log, Safety Management Report Output: Audit Report and potential corrective actions, updated Hazard Log, updated Safety Management Report			

5.3.2 EN 50129:2003, Table E.2 – System requirements specification

(Referred to in EN 50129:2003, 5.3.6)

Table 10 – System requirements specification

Technique / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Separation of safety related systems from non safety-related systems	R: well defined interfaces between safety related systems and non safety-related systems Requirement: focus of risk reduction on safety-related systems and identification of boundary and interfaces Evidence: system safety requirement specification, Preliminary Hazard Analysis identifying safety related and non safety related functions Output: judgement of separation based on Preliminary Hazard Analysis and/or Hazard Analysis		HR: well defined interfaces between safety related systems and non safety-related systems and interface analysis Requirement: focus of risk reduction on safety-related systems and identification of boundary and interfaces Evidence: system safety requirement specification, Preliminary Hazard Analysis identifying safety related and non safety related functions Output: judgement of separation based on Preliminary Hazard Analysis and/or Hazard Analysis	
2. Graphical description including for example block diagrams	HR: Requirement: to identify functional units, subsystems and their relationship Evidence: graphical representation of system Output: judgement of clarity and detail of separation of graphical representation in system description		HR: Requirement: to identify functional units, subsystems and their relationship Evidence: graphical representation of system Output: judgement of clarity and detail of separation of graphical representation in system description	
3. Structured specification	HR: manual hierarchical separation into subtasks, description of the interfaces Requirement: separation of safety, RAM and quality aspects Evidence: structured system requirement specification Output: Judgement of Level of Structure		HR: hierarchical separation using formalised methods, automatic consistency checks, refinement down to functional level Requirement: separation of safety, RAM and quality aspects Evidence: structured system requirement specification Output: Judgement of Level of Structure	
4. Formal or semiformal methods			R: computer-aided Requirement: minimize systematic errors in requirement phase Evidence: Formal or semiformal representation of requirements Output: judgement of the appropriate method used for the system	

Table 10 *(continued)*

Technique / Measures	SIL 1	SIL 2	SIL 3
5. Computer aided specification tools		R: tools without preference for one particular design method Requirement: minimize systematic errors in requirement phase Evidence: Formal or semiformal representation of requirements Output: judgement of the appropriate method used for the system	R: model oriented procedures with hierarchical subdivision, description of all objects and their relationship, common data base, automatic consistency check Requirement: minimize systematic errors in requirement phase Evidence: Formal or semiformal representation of requirements Output: judgement of the appropriate method used for the system
		Requirement: minimize systematic errors in requirement phase Evidence: Formal or semiformal representation of requirements Output: judgement of the appropriate method used for the system	Requirement: minimize systematic errors in requirement phase Evidence: Formal or semiformal representation of requirements Output: judgement of the appropriate method used for the system
6. Checklists	R: prepared checklists for all safety life-cycle phases, concentration on the main safety issues Requirement: completeness of safety processes Evidence: prepared checklists, covering safety life cycle phases addressing critical safety and organisational aspects Output: judgement of completeness of checklists for safety life-cycle phases		R: prepared detailed checklists for all safety life-cycle phases Requirement: completeness of safety and quality processes Evidence: prepared checklists, covering safety life cycle phases addressing critical safety and organisational aspects Output: judgement of completeness of checklists and outcome of application
7. Hazard Log	HR: Hazard Log to be established and maintained throughout the system life-cycle Requirement: structured and comprehensive record of safety-risks, mitigation measures and their status during all life-cycle phases Evidence: paper or electronic Hazard Log Output: judgement on the structure and appropriate application during all life-cycle phases		
8. Inspection of the specification	R: Requirement: verification that all safety, technical and operational requirements are derived correctly		HR: Requirement: verification that all safety, technical and operational requirements are derived correctly
	Evidence: record of inspections carried out		Evidence: record of inspections carried out
	Output: judgement on inspection testing		Output: judgement on inspection testing

5.3.3 EN 50129:2003, Table E.8 – Design phase documentation

(Referred to in EN 50129:2003, 5.2)

Table 11 – Design phase documentation

Technique / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1. Graphical description of sub-systems	HR, SIL 1-SIL 4 Requirement: Description of the contexts and the combines of the subsystems Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with System requirement-specification (as regards content) Output: System requirement-specification			
2. Description of interfaces	HR, SIL 1-SIL 4 Requirement: Complete description of the interfaces (physical, software, environment) Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with system requirement-specification (as regards content) Output: Interface-request-specification, updated requirement-tracing			
3. Environment (EMC, vibrations) studies	R (SIL 1/SIL 2) / HR (SIL 3/SIL 4)· Requirement: Summary of the customer-requests, EN 50126-1 – phase 2, assignment to the standards respectively standardize-classes and formulation of corresponding requirements Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with system requirement-specification (as regards content) Output: System requirement-specification, updated requirement-tracing			
4. Modification procedure	HR, SIL 1-SIL 4 Requirement: Installation of general rules for the action with modifications, care of Hazard log, prosecution and ranking of error messages from the applications Evidence: Audit of manufacturer and users Output: Audit protocols			
5. Maintenance manual	HR, SIL 1-SIL 4 Requirement: Derivation of the maintenance-instructions from the results of the safety case, periods (for example maintenance, inspection, exchange) from MTBF of the modules derives Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with user-documentation (as regards content) Output: Maintenance-handbook, updated requirement-tracing			
6. Manufacturing documentation	HR, SIL 1-SIL 4 Requirement: Installation the manufacture-documentation (for example layout-presentations, montage-instructions, test specifications, programming-rules) under consideration of the results from the safety cases (for example application-rules with modules with inherent fail-safety, manufacturer-rules, subordinate safety cases) Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with user-documentation (as regards content) Output: Manufacture-documentation, updated requirement-tracing			
7. Application Documentation	HR, SIL 1-SIL 4 Requirement: Specifications for the planning, operation, maintenance under consideration of the safety application-conditions (from safety-cases) Evidence: Evaluation in the quality-management-report (qualitative), examination context sensitive with user-documentation (as regards content) Output: User-documentation, updated requirement-tracing			

5.3.4 EN 50129:2003, Table E.10 – Application, operation and maintenance

(Referred to in EN 50129:2003, 5.3.12 and 5.4)

Table 12 – Operation and maintenance

Technique / Measures	SIL 1	SIL 2	SIL 3	SIL 4
1 Production of applications operational and maintenance instructions	R: all operational, application and maintenance instructions traceable back to the design including use of hazard log		HR: all operational, application and maintenance instructions traceable back to the design including use of hazard log	
	Requirement: completeness and correctness of all operational, application and maintenance instructions Evidence: maintenance and operational manual including adequately specified safety application conditions (if any) Output: judgement of completeness and correctness of the manual			
2 Training in the execution of operational and maintenance instructions (see 5.4, Section 5)	HR: initial training of all operators and maintenance staff Requirement: well-skilled maintenance staff Evidence: initial training certificate Output: assessment of staff competence		HR: initial training plus periodic refresher training of all operators and maintenance staff Requirement: well-skilled maintenance staff Evidence: initial training plus periodic refresher training certificate Output: periodic assessment of staff competence	
3 Operator friendliness	HR: the interaction between the person and the system to be as simple as possible, in order to reduce the risk of human errors Requirement: ergonomic HMI (Human Machine Interface) Evidence: easy to understand instructions including interaction in case of failure of system components Output: approval of operational manual			
4 Maintenance friendliness	HR: separate diagnosis tools, safety- related maintenance measures as seldom as possible Requirement: easy-to-use diagnosis tools. Safety related intervention as seldom as possible Evidence: maintenance and diagnosis manual Output: judgement of completeness and correctness of the maintenance manual		HR: sufficient, sensible and simply handled diagnosis tools should be included for unavoidable repairing measures, safety- related maintenance measures as seldom as possible or not necessary at all Requirement: easy-to-use diagnosis tools or system to detect faulty LRU (Least Repairable Unit). Safety-related intervention should be avoided Evidence: maintenance and diagnosis manual Output: judgement of completeness and correctness of the maintenance manual	
5 Protection against operating errors	R: procedural plausibility checks on each input command Requirement: Safe execution on each input command with special focus on safety-critical commands in case of peripheral failures Evidence: Clear description of the procedure for safety-critical commands Output: assessment on the adequacy of the measures taken		HR: procedural plausibility checks on each input command Requirement: Safe execution on each input command with special focus on safety-critical commands in case of peripheral failures Evidence: Clear description of the procedure for safety-critical commands Output: assessment on the adequacy of the measures taken	
6 Protection against sabotage			R: additional organizational measures are necessary Requirement: organizational precautions against unauthorised system access Evidence: access authorization plan or rule Output: assessment of the access authorisation plan with respect to coverage and adequacy of the defined measures	

6 Safety assessment and approval

6.1 Guidance on the concept of Safety assessment

6.1.1 Introduction

The objective of assessment is to arrive at a judgement that the product or the system (subsystem, equipment) is of the defined safety integrity level based on credible evidence and is fit for its intended purpose.

This will include an assessment of the lifecycle processes and their output documents. For this purpose the safety assessor may require additional tests.

It is highly recommended to start and carry out the assessment concurrent to the development process and beyond system acceptance as appropriate as shown in Figure 15. However sometimes it is only necessary to perform final assessment (e. g. if only minor changes are applied to an existing system).

Safety approval is a subsequent stage to assessment and considers the outcome of the judgement arrived at the assessment phase in order to allow the acceptance of implementation or deployment of the product or system. Safety approval is generally given by a safety authority that may employ the outcome of the assessment or additional evidence to arrive at their judgement.

6.1.2 Conditions for the Assessment

In general the safety authority should accept the Safety Assessor or the Safety Assessment Organisation. The safety Assessor could be either a member of the in-house organisation (e.g. Assessment Centre) or an independent external organisation (the criteria for these organisations are defined in EN ISO/IEC 17020). The degree of the independence of the Assessor from the development and RAMS Process should be proven and accepted by the safety authority in charge of the approval. The Assessment organisation should have an accreditation in accordance with EN ISO/IEC 17020.

The assessor should prove as a minimum competence in the following fields:

- specific or relevant expertise in Railway Operation;
- the technology of the system;
- local requirements/rules for application;
- the legal requirements and the recognised rules of the technology;
- the necessary practical experience;
- guarantee for independence and impartiality;
- quality processes in development phase and safety management requirements;
- knowledge of all related CENELEC standards.

Training and sharing of knowledge / experience between assessors is highly recommended.

6.1.3 Phases of Safety Assessment

Table 13 shows assessor activities during the life cycle phases for a safety related product or system development. This table itself is a proposal of how to ensure the appropriate assessor activity. The assessor's output from each phase is generally a documented feedback or report distributed to the parties described in the safety plan. The assessor may additionally generate and deliver examination reports during certain phases covering activities, document structures and analysis.

Table 13 – Typical assessor activity during the life cycle

Phase	Assessors activity
Concept	Review the RAMS principles and Safety Integrity requirements
System definition	— Assess the relevance and completeness of high-level safety requirements and Preliminary Hazard Analysis — Assess the, Safety Plan & Quality Plan — Assess the system boundary, constituents, interfaces with other systems and operational environment — Assess operational concept and normal, degraded, failed and emergency modes — Assess the competency requirements — Assess Data Preparation Plan (if applicable for the system)
Risk analysis	— Assess the risk analysis methods and process — Assess the Risk Tolerability Criteria
System Requirements	— Assess the Preliminary Hazard Analysis is consistent with the Hazards considered in the risk analysis — Assess the system RAM and safety requirements according to: — Testability — Completeness — Clarity — Un-ambiguity — Compliance with standards — Traceability to risk analysis and System definition — Consistency — Assess that interface and environmental requirements are adequately specified — Examine the quality of the specification documents — Assess the quality plan according to: — all planned phases are considered — in each phase appropriate activities are planned and the processes resulting from it are in place — Assess the safety plan according to: — all planned phases are considered — in each phase appropriate activities are planned and the processes resulting from it are in place — Assess the V&V plans according to — traceability between tests and safety requirements — all safety life cycle phases are considered — appropriate measures and activities in each phase were planned consistent with the systems safety integrity level — data preparation and validation plan
Apportionment of System Requirements	— Assess the assumptions made in the apportionment process — Assess the process or methods employed for systematic apportionment — Check Traceability and Consistency to higher level system requirements

Table 13 – Typical assessor activity during the life cycle (*continued*)

Phase	Assessors activity
Design and Implementation	Assess that — Processes, Methods and techniques of system safety plan are applied (also for Subcontractors and suppliers) — the design and architecture documents are up to date, complete and consistent — all planned verification of that system design are done and robust Assess the — Hazard Analysis including operational and interface hazards — Risks arising from newly identified hazards — Risk reduction aspects of the product/system architecture — Generic (Product/Application) Safety Case as appropriate
Manufacture	Assess that — Processes, Methods and techniques of system safety plan are applied (also for Subcontractors and suppliers) — the quality plan requirements have been applied (also for Subcontractors and suppliers)· — the Hazard Log process has been applied — Compliance with mandatory and recommended SIL processes according to Annex E of the standard and other relevant CENELEC standards
Installation	Assess that — the safety application conditions derived from safety analysis and other sources are defined and regarded in the installation manuals and test specifications (if applicable)· — the safety application conditions (if applicable) are applied and records are maintained — in case of migration or transition from an old to a new system, specific safety assessment is performed on the parallel operation
System Validation (Acceptance and Commissioning)	Assess that — every safety requirement is tested, verified and adequately fulfilled — all non-compliances against safety requirements are recorded, assessed and justified and placed in the concluding clause of the safety case — every safety related fault is described and its risks are evaluated and controlled to an acceptable level — the commissioning program describes appropriate activities and processes e.g. change and configuration management — the activities planned for commissioning are fulfilled — all tools used during verification and validation in factory or on site are appropriate for the allocated SIL and used in the correct manner
System Acceptance	Assess that — the Operation and Maintenance manuals include all safety related application conditions and are considered adequate for safe operation and maintenance of the system — all constraints imposed on the system from the operational environment are included in the Operation and Maintenance manuals — all system risks including those relating to operation and maintenance have been adequately identified, controlled and managed — the generic or application specific Safety Case are completed and provide justification for operation of the system — that the operators are adequately trained to cope with normal, degraded, failed and emergency modes

Table 13 – Typical assessor activity during the life cycle (*continued*)

Phase	Assessors activity
Operation and Maintenance	If an Assessors role is continued after acceptance, then he/she should assess that — the essential safety documentation are handed over to the operators or the new project team — the operator/new project team continues to maintain a hazard log — new hazards are recorded, evaluated and their risks are managed — relevance and adequacy of the safety organisation and the staff competencies — the application of the Safety Management Process — maintenance schedule is complied with — assess system maintenance and retrofit Should the Assessors role terminate at the system acceptance stage, then evidence to the satisfactory compliance with above should be provided to the Assessors at the System Acceptance phase. For product/system generic safety cases, the Assessors should satisfy themselves that the above conditions are met when a project is handed over to another project team
Performance Monitoring	If an Assessors role is continued after acceptance, then he/she should assess that — appropriate metrics and Key Performance Indicators (KPI) are collected for safety performance — the performance indicators are aligned with the safety risk targets — Should safety KPIs not indicate compliance with safety targets, a review of the underlying causes and a consultation with the safety authority should be carried out
Modification and Retrofit	If an Assessors role is continued after acceptance, then he/she should assess that — the Impact of any change is risk assessed and managed — there’s a change and configuration management process in place and appropriately applied — adequate records are maintained for version and change history purposes — changes including small changes are assessed for local and global effects In the event of a large scale sub-system change or retrofit including a large number of small changes, parts of the safety process should be repeated from system requirements all the way to system acceptance
Decommissioning and Disposal	When applicable, assess that — the decommissioning is performed according to a plan — the hazards and associated risks of decommissioning are identified and evaluated — appropriate risk control measures are adopted and applied — relevant competencies are catered for during the decommissioning — adequate records are maintained for decommissioning activities — exchange of safety related information takes place with the potential migration project

The following activities should also be carried out, documented and evidence provided to the assessor:

- internal safety audits/reviews;
- internal quality audits/reviews;
- safety participation to design reviews;
- quality participation to design reviews;
- Hazard Log Management;
- change Request Management;
- defect Reporting and Corrective Action.

6.1.4 Contents of the Safety Assessment Report

The safety assessment report should address as an example the following aspects:

- description of assessment process (or e.g. Assessment Plan);
- reference of the assessors or assessing organisation’s authorisation;
- scope and Coverage of Assessment (System Revision, Parts assessed, Reference to System Boundaries and System Interfaces, etc.);
- roles, responsibilities, competencies and independence (Training, Experience, see also e.g. EN 50128:2001, Clause 6, etc.);
- references to relevant documents (Supporting Documents e.g. Safety Cases, Documentation Plan/Configuration Management, Standards, etc.);
- judgement of validation and verification processes applied in the project;
- judgement of the safety analysis process;
- clarification of the safety requirements used for compliance testing;
- the rationale and confirmation that the Safety Requirements are adequately met;
- confirmation that the Criteria for acceptance are met;
- judgement of Methods / Activities (examination of Test Strategy, including justifications for Methods / Activities);
- confirmation that the safety relevant application conditions are met or their management is transferred to the operator / user where appropriate;
- reports about assessors activities as listed in 6.1.3 (Phases of Assessment) including the quality and safety management processes;
- conclusions including restrictions and constraints for use and recommendations.

6.2 Migration strategy from other Standards to CENELEC

6.2.1 Introduction

Frequently an already proven old system should be brought up to the state of the art within the framework of system maintenance. This may be required because of e.g. adaptations in the track layout, innovations in the hardware field or due to the change to a new development environment required within the context of software maintenance.

In such cases the client's expectations/processes and the European regulations often require compliance with the European Standard. The question arises whether and how the proven equipments already approved according to former standards can be integrated into the new or developing subsystems to be approved according to CENELEC. In addition most systems will have interfaces to other systems where safety depends on the use of other standards. In many cases it can also be an advantage to use industrial products based on an already generally accepted safety standard.

In practice a full compliance with EN 50129 / EN 50128 can in general only be established with a complete new system developed in accordance with the requirements of these standards. Even then, some sub-systems may depend on former development practices.

In this section the overall principles and strategies for use or migration of other standards are described.

6.2.2 Differentiation between Systems, Subsystems and Equipment

EN 50129 differentiates between systems, subsystems and equipment. A subsystem is a part of a system and performs a specific function. The exact delimitation of the respective term (system, subsystem, equipment) depends on the application/perspective in a given context and should be defined in a migration project.

An item of equipment is a sub-unit of a subsystem. For example, at the whole railway system perspective, signalling and control constitutes a subsystem and an interlocking is equivalent to an item of equipment. At the signalling system perspective however, an interlocking is a subsystem and the operator console an item of equipment.

According to EN 50129 it is basically allowed to refer in the approval of an application (system, subsystem) to an approval already issued for a universal product or application. Controlling of risks, is possible at system, subsystem or equipment level.

6.2.3 Reuse of System/Subsystem/Equipment

A safety case according to EN 50129 comprises three main parts:

- Quality Management;
- Safety Management;
- Technical Safety Report.

The quality management system (QMS) and safety management process (SMP) are principally aimed at reducing the risks of systematic failures whilst technical safety measures control random failures.

Migration / use of other standards consequently require that both systematic and random failures are controlled in a way that is compliant to EN 50129 and EN 50128.

In many cases, many sub-systems and equipments used in railways comply with other directives because these products have broad range of applications. An example could be PLC's, safety equipment like emergency stops, etc.

Many railways have still parts that comply with older technical standards or rules set forth by the railway administrations. It is important to note that the overall system (application) safety case should be in compliance with EN 50129 but subsystems or equipments can be based on other standards.

For the use of equipment already approved and in service the following conditions for the migration should be fulfilled.

Qualitative safety characteristics can be proved e.g. by reference to

- the approval and proven operation of the system/subsystem/equipment,
- the safety case of the existing system/subsystem/equipment,
- applicable directives of the existing system/subsystem/equipment,
- complied requirements of the respective approval regulations.

The quality management report according to EN 50129 could be provided by

- reference to work processes used in the development (QM system),
- internal and external construction directives,
- used standards relating to the existing system/subsystem/equipment,
- existing documentation of the system/subsystem/equipment, and
- quality requirements met according to the operational experience.

The safety management report according to EN 50129 could be provided by reference to:

- existing safety cases for all equipments of a system/subsystem,
- the verified documentation for all equipments of a system/subsystem,
- the carried-out test of all equipments,
- the approval of all equipments,
- documents describing the difference between the development referential of the existing system and current professional expertise of the already approved system/subsystem/equipment.

In general it may be also possible to consider the existing approved system/subsystem/equipment in the same way as a COTS (see Clause 4 for details).

6.2.4 Safety Case for a New/Developing System/Subsystem/Equipment

The argumentation for the translatability of the results to the new developing system/subsystem/component should be provided in the Safety Plan of that new entity and agreed with the approval authority. The post-qualification of a pre-approved system, subsystem, equipment or component should be made within the framework of the safety case for the new system being developed. Subsystems/equipment without safety case can be used in new developments only if the qualitative characteristics are subsequently proven in a safety case.

6.2.5 Examples of Migration

The cases for safety analysis in a migration project may include

- HW is maintained, new SW is created (SW should be in compliance with EN 50128),
- SW is maintained, HW shall be modified. The development of the HW should be in compliance with EN 50129,
- major modifications on the SW due to the application of EN 50128 without new creation of proven parts. Include proven parts by means of COTS strategy,
- modification of SW development tool chain,
- reuse of proven subsystems/equipments as it is in new EN System/Context.

6.3 Approval for modification and internal adaptation

While the systems (in particular signalling systems) have a comparatively long life cycle, the availability of the equipments on the market is considerably shorter due to the innovation cycle.

This makes it necessary to modify electronic boards already approved. Therefore, for the purposes of compliance with the requirements of EN 50129:2003, 5.5.3, a distinction should be made between

- modifications subjected to the complete procedures of the standard, and
- modifications to which only part of the process/requirements apply.

6.3.1 Conditions

General conditions for any system change:

- the rationale for any change should be documented in a change request;
- any change should result in a new revision/version of the equipment;
- any change should be subject to a documented change management process, which should include a safety impact analysis;

In simple cases (internal adaptation of the component) the approval by the safety authority of the modification of already approved equipment with electronic components can be dispensed with if

- no new Hazards have been introduced (Hazard Analysis has not changed), and
- the Technical Safety Report remains unchanged, and
- the required function of the electronic component is not changed by the adaptation (no modification of specification), and
- the interfaces of the electronic component remain unchanged, and
- an assessment without objections has been carried out by an approved/accredited assessor.

6.3.2 Assessment

The internal adaptation of a component is subject to an assessment by an approved/accredited assessor (see EN 50129:2003, 5.3.9, Subsection 4). In such case a confirmation (and not an Assessment Report) is issued as an output of the assessment.

6.3.3 Information for Safety Authority and Operator

The cases when the safety authority/railway authority has to be informed of an internal adaptation should be agreed with the safety authority and the railway authority. Table 14 shows a possible work split.

Table 14 – Possible Work split Approval for modification

Modification	ISA, Safety Assessment Centre	Safety Regulatory Authority	Railway Authority
Change in the manufacturing process	Acceptance	Information	Information
Component: compatible Component	Acceptance	Information	Information
Component: (Deviation datasheet)	Acceptance	Information	Information
Component: (minor changes)	Acceptance	Information	Information
Bugfixing	Acceptance	Information	Information
Safety Component: compatible Safety Component	Assessment	Approve	Information
Change of SRS / Functions	Assessment	Approve	Information
Change of Safety Case	Assessment	Approve	Information

Annex A
(informative)

EN/IEC standards for safety analysis

NOTE For each guide the description text comes from the IEC internet site.

EN 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology* (IEC 60300-3-1)

Gives a general overview of commonly used dependability analysis techniques. It describes the usual methodologies, their advantages and disadvantages, data input and other conditions for using various techniques. It is an introduction to selected methodologies and is intended to provide the necessary information for choosing the most appropriate analysis methods.

EN 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* (IEC 60812)

Describes Failure Mode and Effects Analysis (FMEA) and Failure Mode, Effects and Criticality Analysis (FMECA). Gives guidance as to how they may be applied:

- by providing the procedural steps necessary to perform an analysis;
- by identifying appropriate terms, assumptions, criticality measures, failure modes;
- by determining ground rules;
- by providing examples of the necessary forms.

EN 61025, *Fault tree analysis (FTA)* (IEC 61025)

Defines basic principles, provides the steps necessary to perform an analysis, identifies appropriate assumptions, events and failure modes, and provides identification rules and symbols.

EN 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods* (IEC 61078)

Describes procedures for modelling the dependability of a system and for using the model in order to calculate reliability and availability measures. The RBD modelling technique is intended to be applied primarily to systems without repair and where the order in which failures occur does not matter. For systems where the order of failures is to be taken into account or where repairs are to be carried out, other modelling techniques, such as Markov analysis, are more suitable.

EN 61165, *Application of Markov techniques* (IEC 61165)

Not only are Markov analysis methods suited to the modelling of maintenance strategies, but such methods also enable the failure restoration events to be modelled in a pictorial way which is in itself a valuable feature.

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

Provides a guide for HAZOP studies of systems utilizing the specific set of guide words defined in this standard. Also gives guidance on application of the technique and on the HAZOP study procedure, including definition, preparation, examination sessions and resulting documentation and follow-up.

Annex B
(informative)

Documentation for approval

B.1 Introduction

The purpose of this Annex B is to give an example, in a standardized manner, of the documents to be issued for the proper management of the approval process for “Generic Products”, “Generic Applications” and “Specific Applications”, in compliance with EN 50129 (and the related EN 50126-1).

This Annex should be used whenever it is necessary to perform the approval of “Generic Products”, “Generic Applications” and “Specific Applications” consisting of electronic products and/or systems for signalling.

The structure of the lifecycle is illustrated in EN 50129:2003, Figure 4.

It should be specified that phases 1 to 4 have been duplicated in Table B.1, as these phases have to be carried out by both the Railway Authority and the Supplier (depending on the application); moreover, the Railway Authority is responsible for phases 11 to 14, but the documentation (especially under phase 13) are in charge of the Supplier. The sequence for performing the first four phases (Railway Authority and Supplier), need not necessarily be carried out according to the sequence shown in Table B.1, depending on the case.

Table B.1 contains a list of the documentation that is to be produced during the various phases of the lifecycle defined in EN 50129:2003, Figure 4. The number of documents to be produced may vary depending on the system’s complexity and on the applications. Therefore, in the case of non-complex systems, several documents may be combined into one (however, in documents containing several documents in one, the same requirements should hold and be applied as for individual documents), whereas, in the case of very complex systems, the documents may be divided into a set of handier documents, organized according to a hierarchical structure.

Taking into account the above, each line in Table B.1 is assigned with a number for traceability reasons. The numbering criteria are as follows. The Document No. is constituted of two figures separated by a point. The first and the second figures represent respectively the number of the corresponding EN 50126-1 phase which the document belongs to and a progressive number. The table itself is only one example, just to remember that such a table is a useful tool to be tailored on the Project and which can differ a bit from Project to Project. For instance, where similar documents can be provided both by Customer (or Railway Authority) and Supplier(s), one suggestion is to put a letter (e.g. “S” for Supplier, “C” for Customer, and so on), in separate lines of the table, before the document number, as this can be equal for the same EN 50126-1 corresponding phase applied to the different actors in the Project.

In addition, a detailed Project Documentation Plan shall be provided as either a separate document or embedded in other Plans, where the traceability and the responsibility of the document issuing shall be clarified.

B.2 Documentation table structure

The correct function of each phase within this document is defined below.

Table B.1 contains a list of all the documents required for performing the approval process for a “Generic Product “Generic Application” or “Specific Applications and includes the following information fields:

Document No. Phase No. * Document No.

EN 50126-1 Phase “Lifecycle ” phase described in Standard EN 50126-1

Document name Title of document

EN 50126-1 reference Paragraph in which EN 50126-1 specifically refers to the document (or the related activity).

EN 50129 reference Paragraph in which EN 50129 specifically refers to the document (or the related activity).

Purpose Explanation of the goals the document is aiming at

Notes General notes regarding the document

B.3 Liaison to EN 50129:2003, 5.5.2

This Annex B makes reference to EN 50129:2003, 5.5.2, and consider the approval mainly in the sense of the Railway Authority Approval. That implies that the content of Annex B is to be tailored on the specific Project or Application. Moreover, depending on the application, different regulatory approval conditions may apply.

Table B.1 – Documentation for Approval

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
1.1	1	Railway Authority Concept Document	6.1	-	It describes the overall system basic goals, necessary for the development of the following phases of the lifecycle. It defines the overall justification about the economical, technical and safety aspects of the project	
2.1	2	Overall System Specification (General, Functional and RAMS)	6.2.3.1, 6.2.3.2, 6.2.3.3	-	It defines the activities to be developed and the phases of the development, reflecting the Customer view. For each phase the activities, the responsibilities and the documents are defined. This document allows a monitoring of the activity progress, both to the Customer and the Supplier. The Documentation Plan may be a separate document or included in this plan	See Annex C
2.3	2	Customer Development Plan	5.3.4	-		May be integrated with the Preliminary Safety Plan (R2.2)
2.5	2	Quality Plan	5.3.5 d)	5.2	This document should cover the Railway Authority scope of work covering the aspect defined in EN 50126-1:1999, 6.2.3.4. It describes the activities required to identify, evaluate and eliminate/controls the hazards or reduce the associated risk to an acceptable level	
2.2	2	Preliminary Safety Plan	6.2.3.4	-		May be integrated into the Quality Plan (R2.5)
2.4	2	Assessment Plan (System / HW / SW)	-	-		
3.1	3	Risk Analysis	6.3.3.1, 6.3.3.2	A.4.1		
3.2	3	Hazard Log	6.3.3.3	-		
4.1	4	System Requirements Specification	6.4.3.1	-	It describes and documents: — Functional — Non-Functional — RAMS — Interfaces — Constraints — Physical/Technological requirements for the project development	Annex C of the Application Guideline gives an example of a structure of the system requirements specification

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
1.1	1	Feasibility Study	6.1.3.2	-		
2.1	2	System Specification (Preliminary)	6.2.3.1	-		
2.3	2	Supplier Development Plan. (SYS/HW/SW)	-	-	It defines the activities to be developed and the phases of the development, reflecting the Supplier view. For each phase the activities, the responsibilities and the documents are defined. This document allow a monitoring of the activity progress, both to the Customer and the Supplier	
2.4	2	Quality Plan	5.3.5 d)	5.2		It will also include, among others, coverage of all activities regarding Design Reviews, Traceability, Checklists, etc.
2.2	2	Safety Plan	6.2.3.4	5.3.4		
2.5	2	Configuration Management Plan (HW/SW)	-	5.2		
2.6	2	Preliminary Hazard Analysis	-	Table E.6, Row 1		It may be included in “Hazard Analysis”
3.1	3	Hazard Analysis (FTA – Causal analysis)	6.3.3.1	A.4.3	…. It will include the Preliminary Hazard Analysis	
3.2	3	Hazard Log	6.3.3.3	5.3.5		Database format
4.1	4	(Final) System Specification, Includes SAD (System Architecture Description)	6.4.3.1	5.4, Section 2-2.1		
4.2	4	Functional and Safety Requirements Specification	6.4.3.1	5.3.6 Clause A.2		

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
4.3	4	RAM Requirements Specification (if not included in F4.2)	6.4.3.1	-		
4.4	4	Verification and Validation Plan (System/Hardware/ Software)	6.4.3.2	5.3.9		(More than one document may be prepared, if necessary)
4.5	4	System Test Specification (Functional, Safety, other systems interface)	6.4.3.2	5.4, Section 2		
4.6	4	RAM Plan	6.4.3.3	-		
4.7	4	Documentation Plan	-	-		Complete list of all system documents (those already issued and to be issued)
4.8	4	Report of Verification of System Requirements and Architecture	-	-		
5.1	5	Subsystem Specification	6.5.3.1	5.4, Section 2-2.1		
5.2	5	Subsystems Functional and Safety Requirements Specification. Includes SAD (System Architecture Description for Subsystems)	6.5.3.1	Clause A.2		To be drawn up only if not included in the Phase 4 document

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
5.3	5	Subsystems RAM Requirements Specification (if not included in F5.2)	6.5.3.1	-		To be drawn up only if not included in the Phase 4 document
5.3	5	Subsystem Test Specification (Functional, Safety, other system interface)	6.5.3.2	5.4, Section 2		To be drawn up only if not included in the Phase 4 document
5.4	5	System FMEA Analysis (SFMEA)	-	B.3.1, Note		Proof of achievement of the Hazardous Failure rate value according to the SIL level
5.5	5	Report of Verification of Subsystem Requirements and Architecture	-	-		
6.0	6 – HW Design	HW Requirements Specification	6.6.3.1	5.3.7		
6.1		System/LRU design documents. The following documents should be provided separately, as a minimum: Functional Description; Safety Analysis; Electrical Diagram; Block Diagram; Materials List; Assembly Documents; Test Procedure	6.6.3.2	5.3.7		

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
6.2	6 – HW V&V	LRU Test Specification	6.6	5.4, Section 2		(as far as applicable)
6.3		LRU Test Report	6.6	5.4, Section 2		
6.4		LRU Failure Test Plan	6.6	5.4, Section 2, Annex C		
6.5		Failure Test Report	6.6	5.4, Section 2, Annex C		
6.6		Hardware Validation Report (Test results versus requirements)	6.6	-		
6.30	6 – HW-SW Integration (Design)	HW-SW Integration Test Plan	6.6	-		
6.31		HW-SW Integration Test Report	6.6	-		
6.33	6 – System Integration (Design)	System Configuration	6.6.3.2	-		

6.34		System design documents: Inter-connections diagram;
		Block diagram;
		Materials list;
		Assembly documents;
		Test procedure
			6.6.3.2	-		

6.35	6 – System Integration (V&V)	Type Tests Plan	-	5.4, Section 4, Clause B.4		
6.36		Type Tests Report	-	5.4, Section 4 Clause B.4		
6.37		Intermediate RAM Report	6.12.3.2	-		
6.38		System/Subsystem Test Report	-	-		

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
6.39	6 – Integration (Design)	Installation Manual	6.6.3.3	Table E.8, Row 7		
6.40		User's Manual	6.6.3.3	Table E.10		
6.41		Maintenance Manual	6.6.3.3	Table E.8, Row 5		
6.42		Manufacturing and Inspection Plan	6.7	Table E.8, Row 6		
6.43		Installation Plan (of the first experimental Specific Application)	6.7	-		
6.44		Commissioning and Putting-into-service Plan (of the first experimental Specific Application)	6.7	-		
6.45		Safety case for Generic Application or Generic Product	6.6.3.5	5.1 – 5-5	Implementation of EN 50129:2003, 5.1-5.5. As a minimum, this document acts as a synthesis of the "Conditions for Safety Acceptance and Approval", and will include all the links to all the specific documents covering the different aspects, principally: — Evidence of Quality Management (documents constituting QMR) — Evidence of Safety Management (documents constituting SMR) — Evidence of Functional and Technical Safety (documents constituting TSR)	
7.2	7	Test Report for the manufactured systems	6.7	-		
8.1	8	Installation Reports	6.8.3.1 – 6.8.3.2	-		
8.2	8	Customer Training Courses Plan	6.8.3.4	Table E.10, Row 2		

Table B.1 - Documentation for Approval *(continued)*

Document No	EN 50126-1 Phase	Document name	References		Purpose	Notes
			EN 50126-1:1999	EN 50129:2003		
9.1	9	Final Validation Report (Supplier internal document)	6.9.3.1	-		
9.2	9	Technical file for “CE Stamping	-	-		For Generic Products only
9.3	9	Field Validation Test Plan (experimentation)	6.9.3.2	-		
9.4	9	Field Test Validation Report (experimentation)	6.9.3.2	-		
9.5	9	Safety case for the first experimental Specific Application (if required)	6.9.3.3	5.1 – 5.5		
10.1	10	“Functional Assessment” Report	6.10.3.1			
10.2	10	“Safety Assessment” Report	6.10.3.1			
10.3	10	“Overall Assessment” Report	6.10.3.1			
10.4	10	Certificate of Homologation	6.10.3.2			
11.1	11	Setting up of FRACAS	6.11.3.1			
12.1	12	Periodic Test Plan	6.12.3.1			For preventive maintenance
12.2	12	Final RAM Report	6.12.3.2			
13.3	13	System Modification Plan (after homologation)	6.13.3.2			
14.1	14	System Disassembling and Decommissioning procedure	6.14.3.1			

Annex C
(informative)

Structure of the System Requirements Specification

C.1 Part one – General information

C.1.1 Purpose

A synthetic definition is to be given of the objective one wishes to achieve through the document's drafting.

(Example: The purpose of this document is to specify the functional and RAMS requirements for the system being considered, in order to permit the correct development of the subsequent phases of the "Life Cycle").

C.1.2 Scope

It is necessary to specify the system to which the document is applicable, and for which railway transport sector said system will be used.

(Example: This document is applicable exclusively to the development of the XYZ system, which will be used in the "Signalling" sector).

C.1.3 Related documentation

It is necessary to list the documents (standards, laws, regulations, specifications, etc.) that are used as reference and/or that support the information contained in the document. Each document cited has to contain: a number placed in square brackets, which will be indicated as reference within the document; the complete version or revision code, or date of issue; the complete title as it is in the language in which the document was written.

C.1.4 Definitions and abbreviations

It is necessary to list the definitions and abbreviations recurring most frequently in the text, and which facilitate comprehension of the document.

C.2 Part two – Requirements

C.2.1 Input elements

It is necessary to specify the documents deriving from phases 1, 2 and 3 of the Life Cycle and/or all the documents and the basic data necessary for the correct development of activities.

C.2.2 System definition

It is necessary to define the system, including the system's objectives and boundaries.

C.2.3 Mission profile

It is necessary to define the system's maximum operational performance requirements (for example: continuous service, max number of demands/operations per day/hour, etc.).

C.2.4 Functional requirements

It is necessary to define the functions that the system has to carry out, including limit or nominal values.

C.2.5 RAM requirements

For each function carried out by the system, it is necessary to define (if required) the RAM values (or strategies or architectures) that the system has to meet and fulfil.

C.2.6 Safety requirements

For each safety function carried out by the system, it is necessary to define the safety requirements for that function along with the safety integrity level with which the function has to be designed and developed.

C.2.7 Diagnostics requirements

It is necessary to define the requirements for the diagnostics functions (e.g. system log and error detecting), used to improve the maintainability and, consequently, the availability of the system.

C.2.8 Logistics support requirements

It is necessary to define the requirements for the (human, technological, instrumentation) resources which are to be used for system development.

C.2.9 Interface requirements

It is necessary to define the interfaces between the system and other systems to which it will be connected (including voltage levels, communication protocols, etc.).

C.2.10 Operating environment

It is necessary to define the operating environment in which the system will be installed, with reference to the relevant ENs concerning this subject.

Bibliography

The following documents were consulted during the preparation of this Application Guideline in addition to the references listed in Clause 2 and Annex A.

EN 61703:2002, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms* (IEC 61703:2001)

IEC/TR 62380, *Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment*

IPC-A-610, *Acceptability of Electronics Assemblies Training and Certification Program*

ISO 19011:2002, *Guideline for quality and/or environmental management systems auditing*

IRSE-Report, *Proposed Cross Acceptance Processes for Railway Signalling Systems and Equipment (26.02.2003)*

MIL HDBK 217F, *Military Handbook – Reliability prediction of electronic equipment (Notice 2 – 1995)*

EUROCAE ED 80, *Design Assurance Guidance for Airborne Electronic Hardware*

Danish Railway Inspectorate Guide, *Approval of electronic systems for signalling (15.01.2002)*

Questionnaire on Cross Acceptance, prepared by CLC/SC 9XA Italian National Committee (09.12.2003)

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Copyright subsists in all BSI publications. BSI also holds the copyright, in the UK, of the publications of the international standardization bodies. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Manager.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™