

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.

© BSI 2010

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
----------	------	---------------

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

© 2009 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Ref. No. CLC/TR 50506-2:2009 E

 **Documents**
Document Sharing Hub

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

Page

Introduction	5
1 Scope	6
2 References	6
3 Terms, definitions, symbols and abbreviated terms	7
3.1 Terms and definitions	7
3.2 Symbols and abbreviated terms	8
4 Safety design for signalling subsystems	10
4.1 Safety principles	10
4.2 Components development guideline	19
4.3 Specific implementation examples	25
5 Safety case structure in relation with associated documents and activities	28
5.1 Introduction	28
5.2 Safety Case for Signalling Systems	28
5.3 Recommendations regarding the fulfilment of the requirements of tables in EN 50129:2003, Annex E	62
6 Safety assessment and approval	68
6.1 Guidance on the concept of Safety assessment	68
6.2 Migration strategy from other Standards to CENELEC	73
6.3 Approval for modification and internal adaptation	75
Annex A (informative) EN/IEC standards for safety analysis	77
Annex B (informative) Documentation for approval	78
B.1 Introduction	78
B.2 Documentation table structure	79
B.3 Liaison to EN 50129:2003, 5.5.2	79
Annex C (informative) Structure of the System Requirements Specification	87
C.1 Part one – General information	87
C.2 Part two – Requirements	87
Bibliography	89

Figures

Figure 1 – Example for hierarchical composition of Functional units	11
Figure 2 – Example for creation and manifestation mechanisms of faults, errors, and failures.....	11
Figure 3 – Example for the mechanisms of ‘fundamental chain’	12
Figure 4 – Relationships of faults, errors and failures	12
Figure 5 – Representation for failures of single and multiple natures	14
Figure 6 – Inherent fail safe devices structure and associated threats	15
Figure 7 – Composite fail safe devices structure and associated threats	17
Figure 8 – Reactive fail safe devices structure and associated threats	18
Figure 9 – Example of composite fail-safety with identical VLSI components	21
Figure 10 – Example of reactive fail-safety with different VLSI components	23
Figure 11 – Example of development process for VLSI components (FPGA, EPLD, etc.).....	25
Figure 12 – Example of overall Safety Cases structure	30
Figure 13 – Structure of the Technical Safety Report	46
Figure 14 – Example of inherent fail-safety	50
Figure 15 – Example for Relation between Design Functional Breakdown	55
Figure 16 – Example of Relation breakdown from FMEA to FTA	56
Figure 17 – SRAC classification	58
Figure 18 – Exported constraints and SRAC management	59

Tables

Table 1 – Examples for single and coupled failures types	14
Table 2 – Guidance for threats mitigation in inherent fail-safe devices.....	16
Table 3 – Guidance for threats mitigation in composite fail-safe devices	17
Table 4 – Guidance for threats mitigation in reactive fail-safe devices	18
Table 5 – Example of documentation linked to Quality Management	32
Table 6 – Typical Example of some Safety Activities in the Lifecycle	36
Table 7 – Methods for Safety Analysis	37
Table 8 – List of safety methods and reference Standards.....	37
Table 9 – Safety planning and quality assurance activities.....	63
Table 10 – System requirements specification.....	64
Table 11 – Design phase documentation	66
Table 12 – Operation and maintenance	67
Table 13 – Typical assessor activity during the life cycle.....	69
Table 14 – Possible Work split Approval for modification	76
Table B.1 – Documentation for Approval.....	80

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).

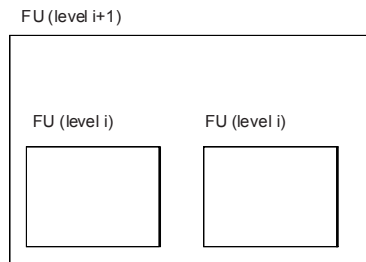


Figure 1 – Example for hierarchical composition of Functional units

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

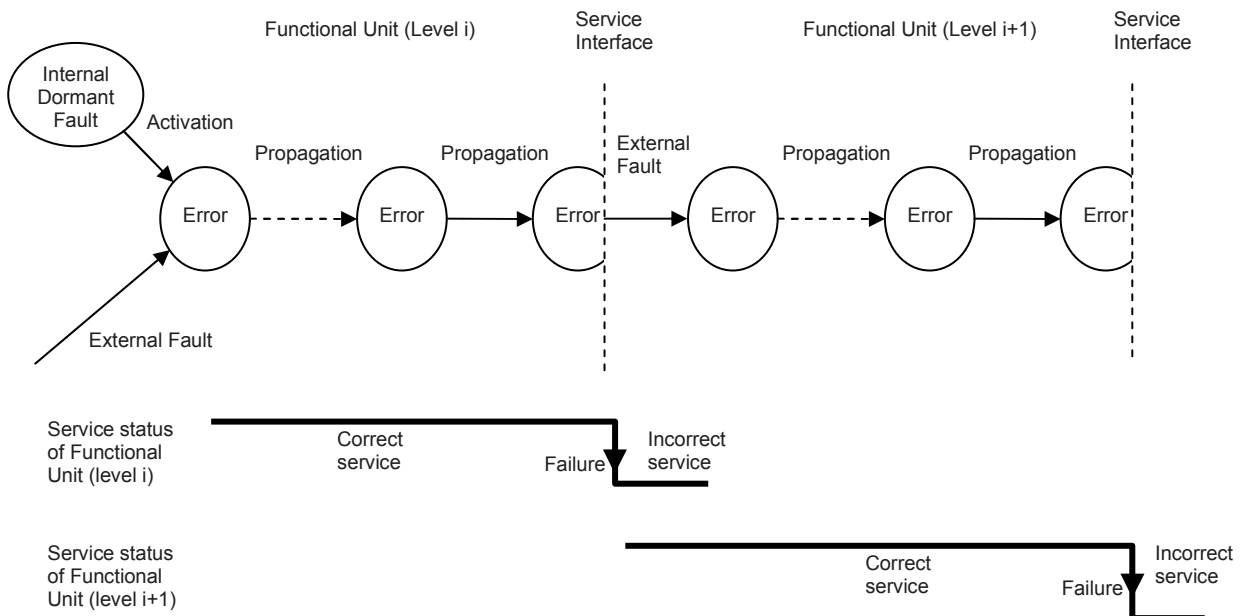


Figure 2 – Example for creation and manifestation mechanisms of faults, errors, and failures

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.

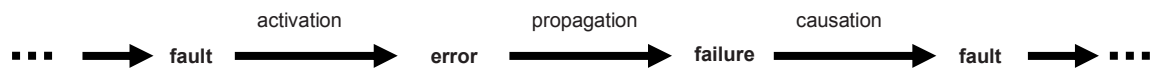


Figure 3 – Example for the mechanisms of ‘fundamental chain’

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.

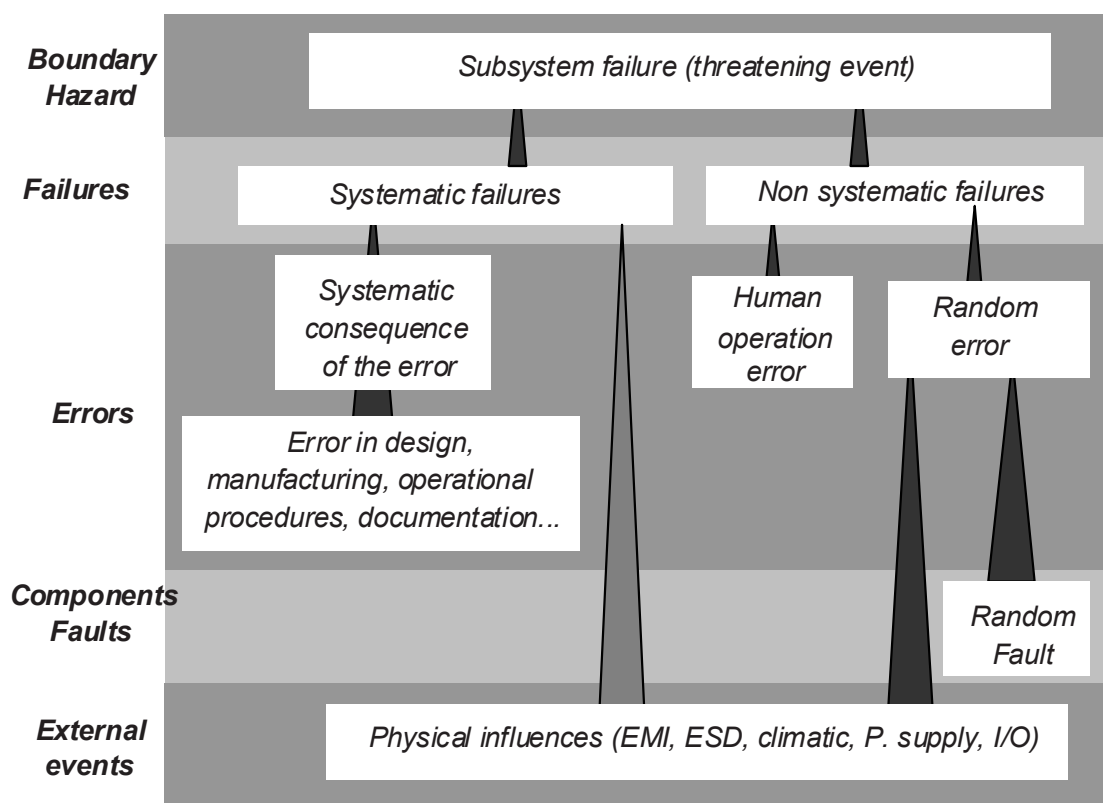


Figure 4 – Relationships of faults, errors and failures

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 monoprocesor 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 monoprocesor 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).

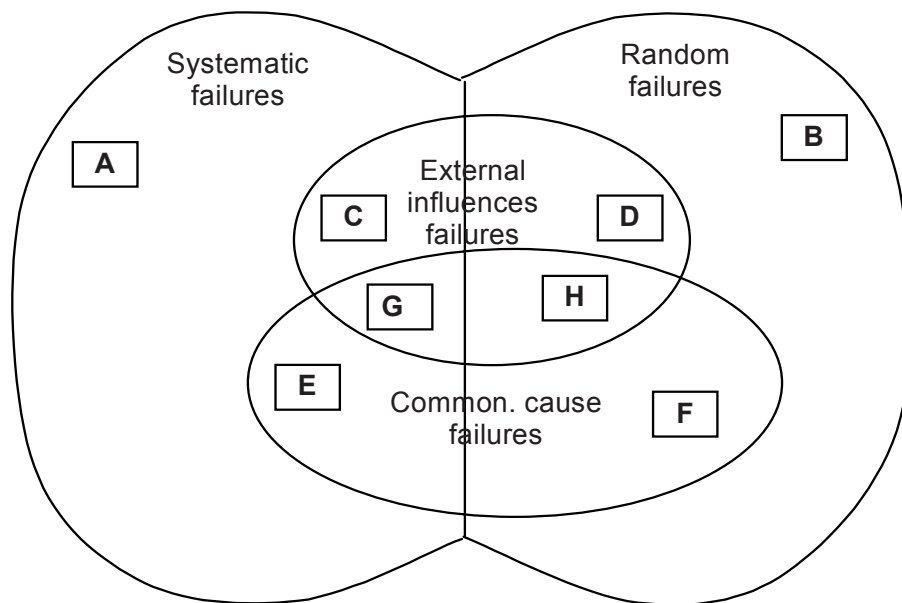


Figure 5 – Representation for failures of single and multiple natures

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).

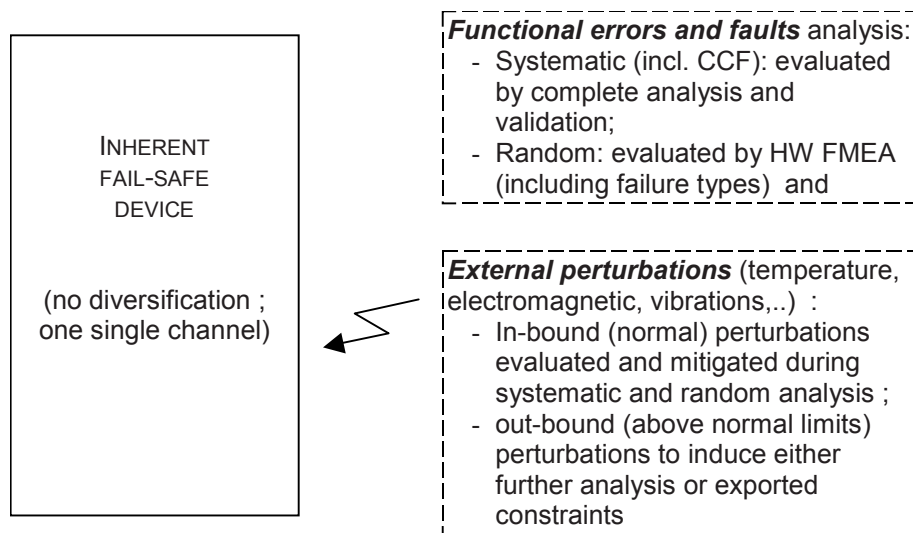


Figure 6 – Inherent fail safe devices structure and associated threats

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.

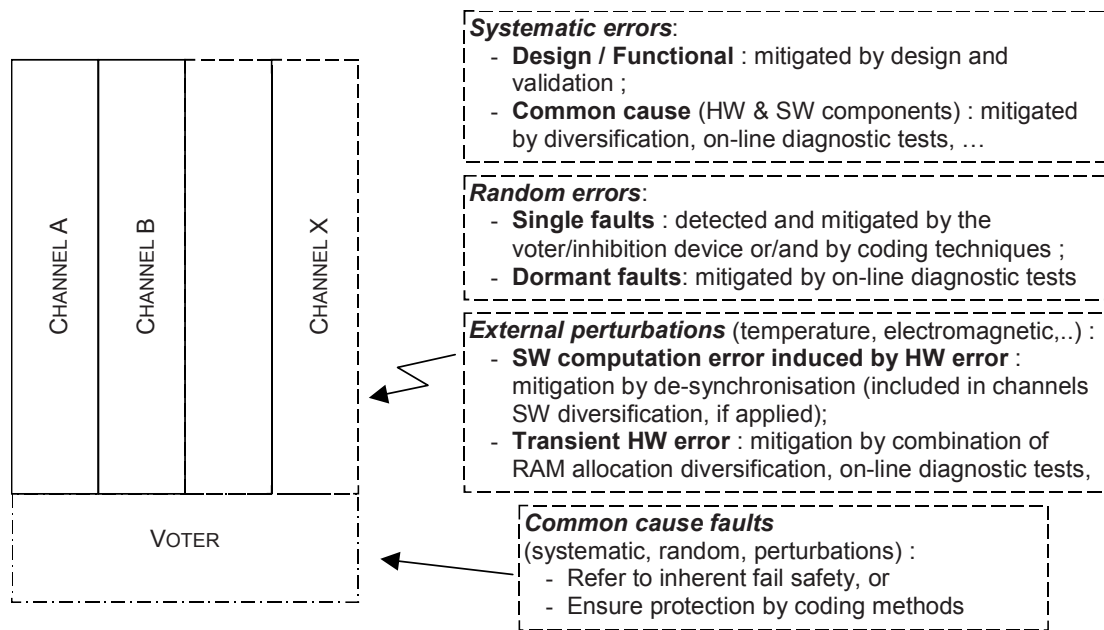


Figure 7 – Composite fail safe devices structure and associated threats

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 μ P 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.

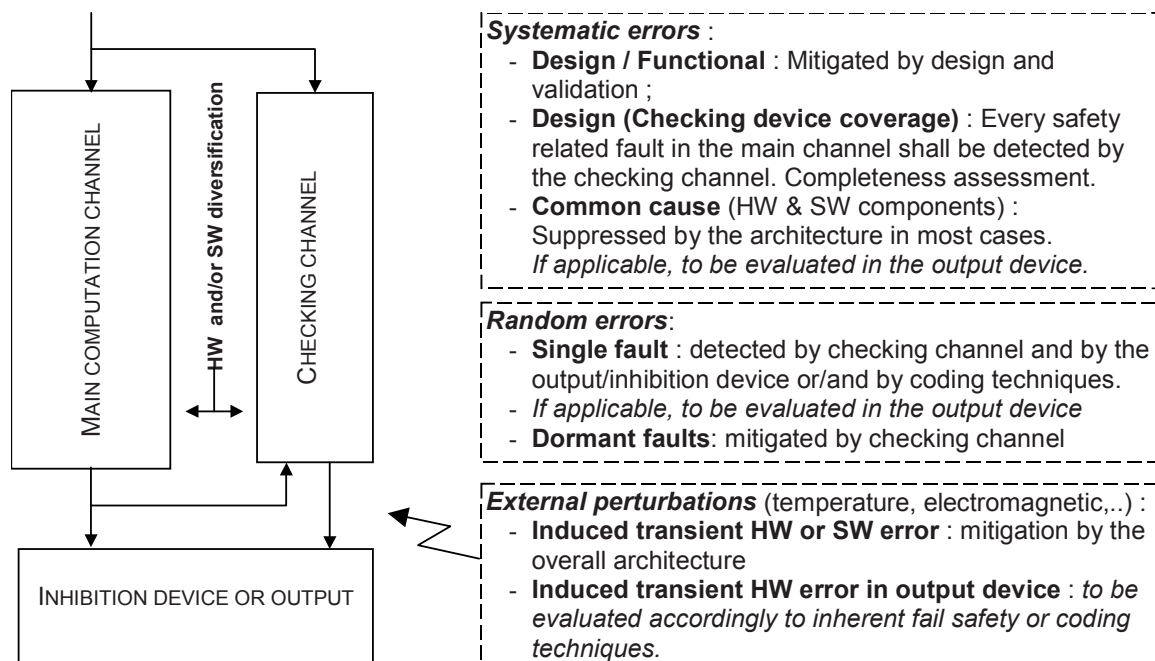


Figure 8 – Reactive fail safe devices structure and associated threats

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.

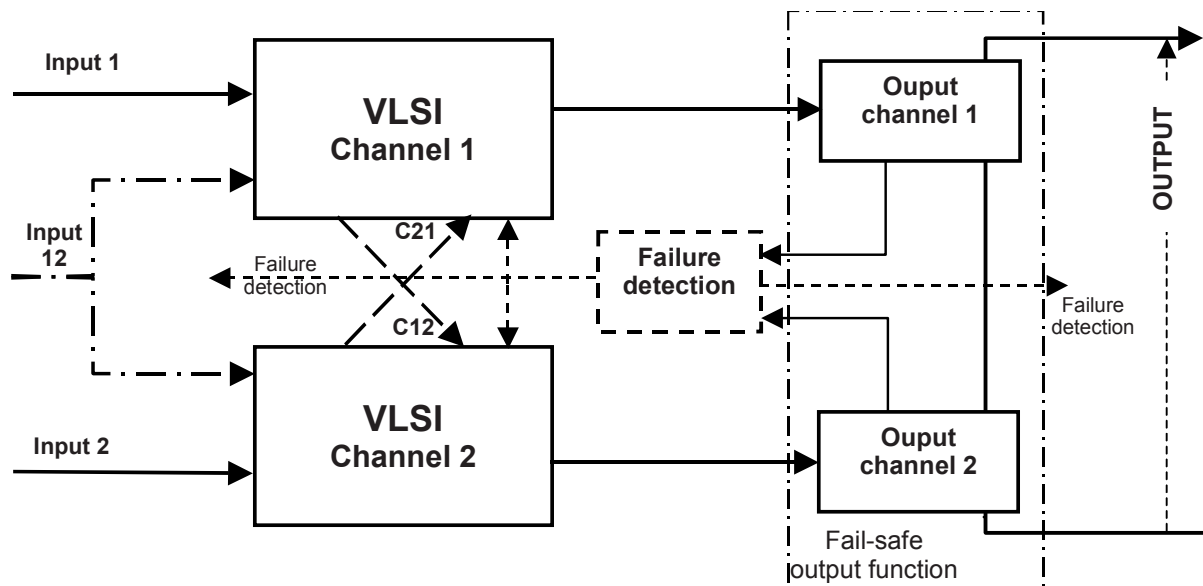


Figure 9 – Example of composite fail-safety with identical VLSI components

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.

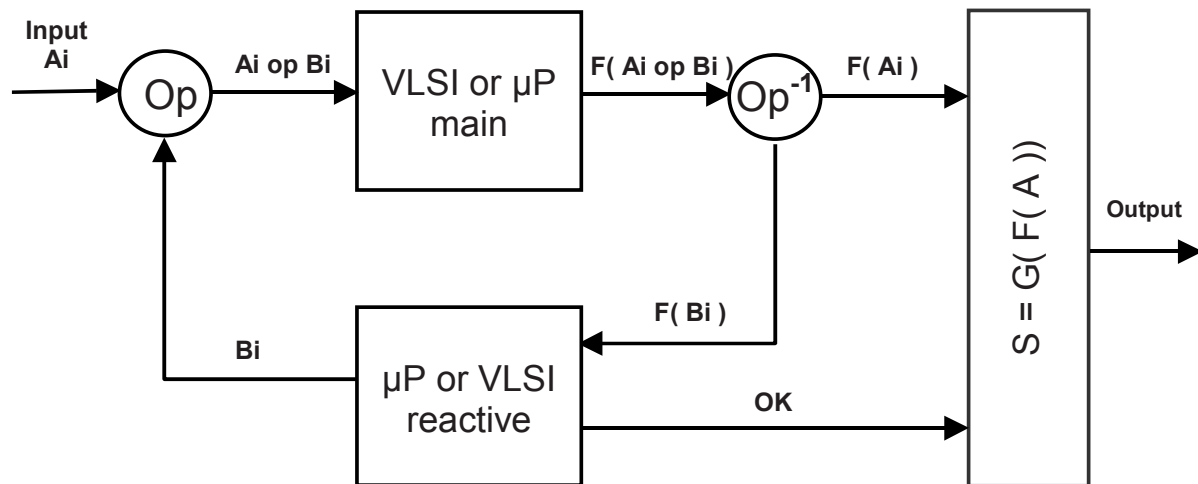


Figure 10 – Example of reactive fail-safety with different VLSI components

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.

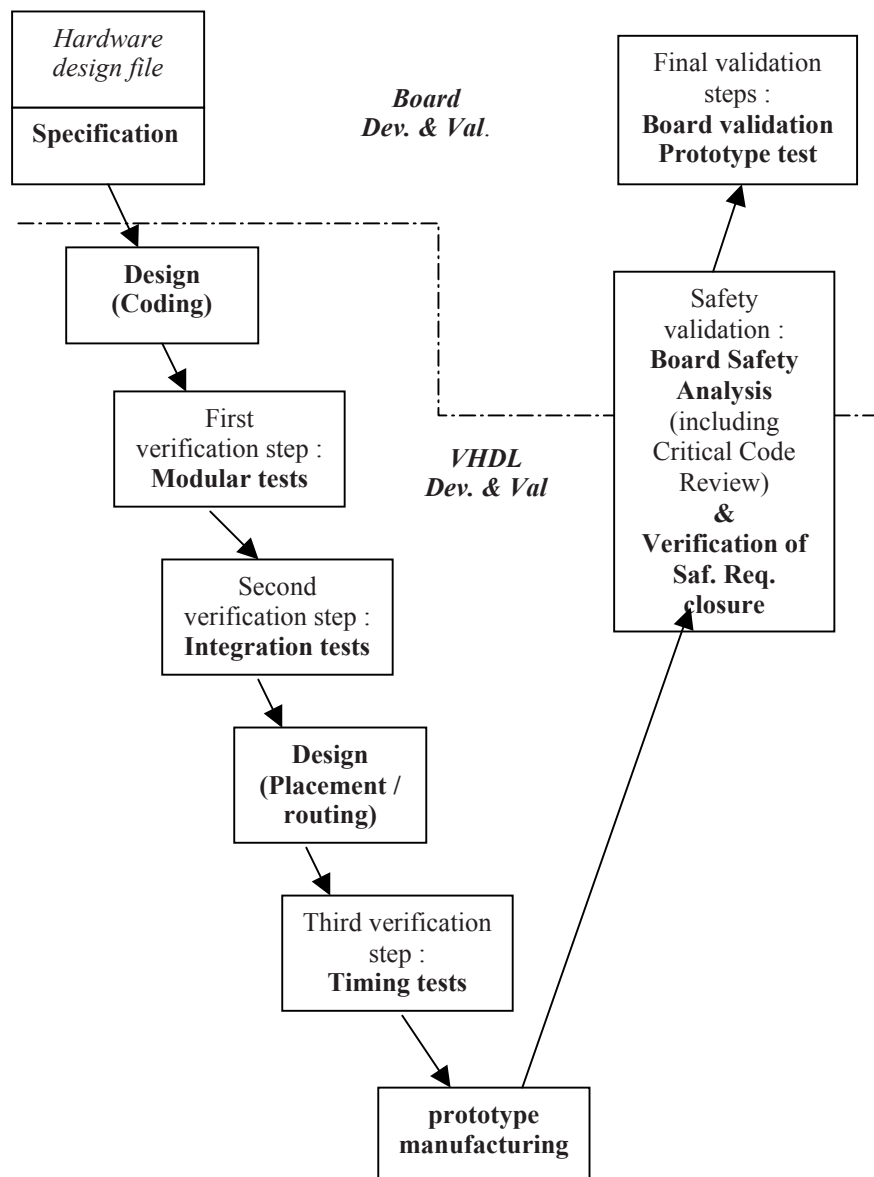


Figure 11 – Example of development process for VLSI components (FPGA, EPLD, etc.)

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.