SLOVENSKI STANDARD
SIST-TP CLC/TR 50506-2:2010

01-februar-2010

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Vodilo za uporabo EN 50129 - 2. del: Zagotavljanje varnosti

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

Ta slovenski standard je istoveten z: **CLC/TR 50506-2:2009**

ICS:

35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST-TP CLC/TR 50506-2:2010 **en**

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

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

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

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).

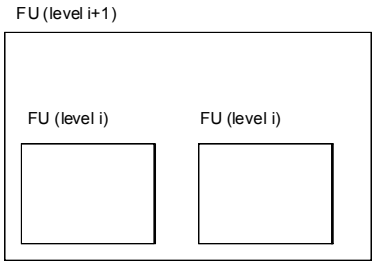

Figure 1 – Example for hierarchical composition of Functional units

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

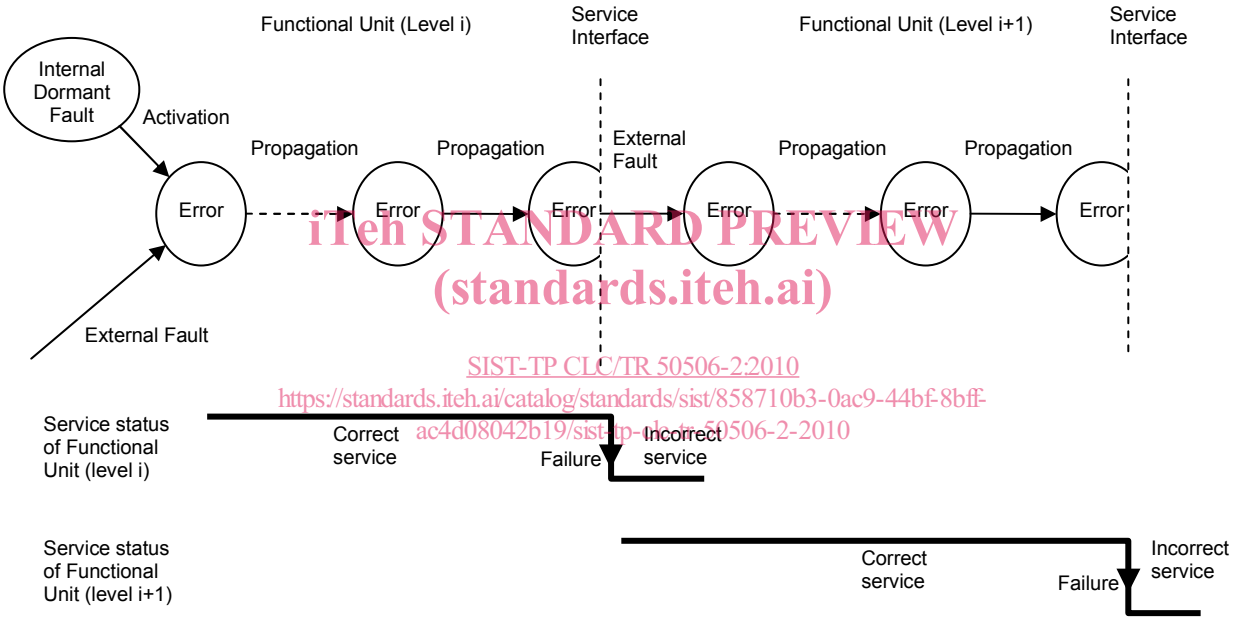

Figure 2 – Example for creation and manifestation mechanisms of faults, errors, and failures

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.

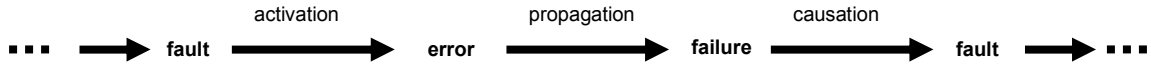

Figure 3 – Example for the mechanisms of 'fundamental chain'

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.

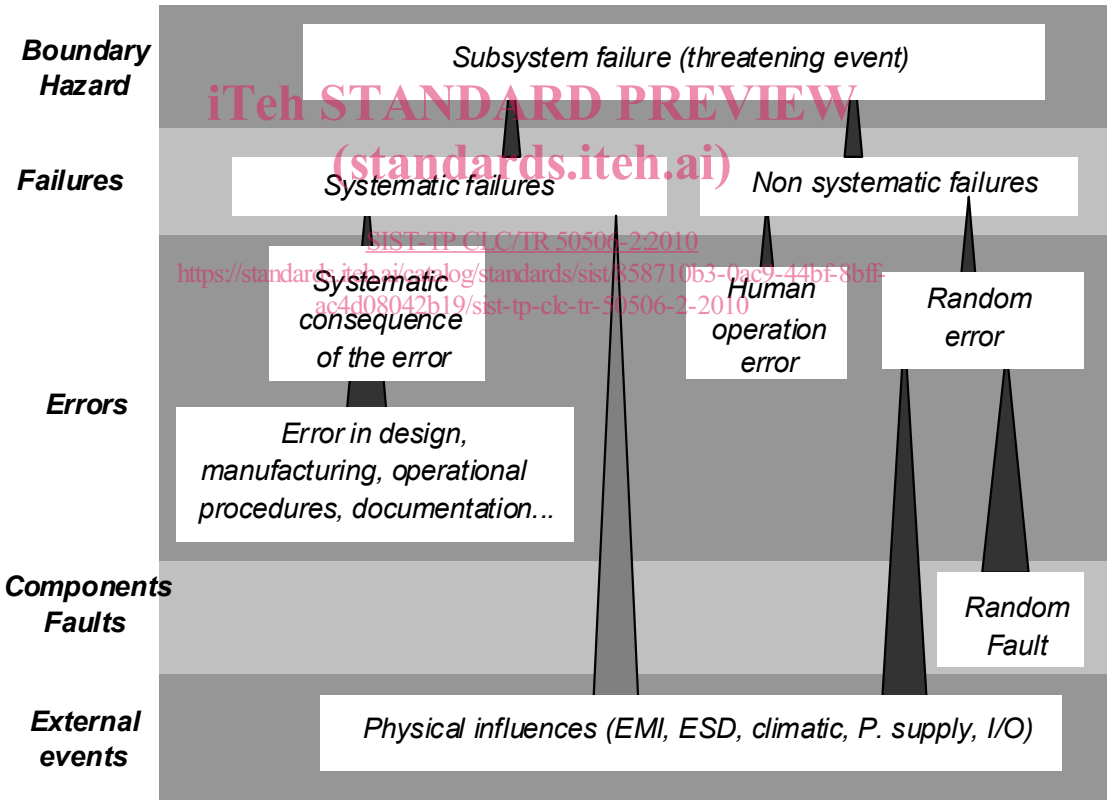

Figure 4 – Relationships of faults, errors and failures

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.