SLOVENSKI STANDARD
oSIST prEN 50129:2017

01-februar-2017

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Signalno-varnostni elektronski sistemi

Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist-cfr-50129-2019

Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation

Ta slovenski standard je istoveten z: **prEN 50129:2016**

ICS:

35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50129:2017 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

oSIST prEN 50129:2017

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50129

December 2016

ICS 93.100

Will supersede EN 50129:2003

English Version

Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2017-02-24.

It has been drawn up by CLC/SC 9XA.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German).
A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

SIST EN 50129:2019
en-50129-2019

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2016 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Project: 60242

Ref. No. prEN 50129:2016 E

oSIST prEN 50129:2017

Contents

Page

European foreword **5**
Introduction **6**
1 Scope **7**
2 Normative references **8**
3 Terms ,definitions and abbreviations **8**
3.1 Terms and definitions 8
3.2 Abbreviations 15
4 Overall framework of this standard **16**
5 Requirements for developing safety-related electronic systems **18**
5.1 Introduction 18
5.2 The quality management process 18
5.3 The safety management process 19
6 Requirements for elements external to the lifecycle **29**
6.1 Introduction 29
6.2 Re-use of pre-existing items 29
6.3 Safety-related tools for electronic systems 31
6.4 Physical security and IT-Security 32
7 The Safety Case: structure and content **33**
7.1 The Safety Case structure 33
7.2 The Technical Safety Report 35
7.3 Different kind of Safety Cases 42
7.4 Provisions for the Specific Application Safety Case 42
7.5 Dependencies between Safety Cases 43
8 System safety acceptance and subsequent phases **44**
8.1 System safety acceptance process 44
8.2 Operation, maintenance and performance monitoring 47
8.3 Modification and retrofit 47
8.4 Decommissioning and disposal 47
Annex A (normative) **Safety Integrity Levels** **48**
A.1 Introduction **48**
A.2 Safety requirements **48**
A.3 Safety integrity **49**
A.4 Determination of safety integrity requirements **49**
A.4.1 General 49
A.4.2 Risk Assessment 51
A.4.3 Hazard Control 52
A.4.4 Identification and treatment of new hazards arising from design 56
A.4.5 An example of THR/TFFR/FR and SIL allocation 57

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

oSIST prEN 50129:2017

A.5 Assignment of SILs **59**
A.5.1 General aspects 59
A.5.2 Relationship between SIL and associated TFFR 60
Annex B (normative) **Management of faults for safety-related functions** **61**
B.1 Introduction **61**
B.2 General concepts **61**
B.2.1 Detection and negation times 61
B.2.2 Composition of two independent items 62
B.3 Effects of faults **63**
B.3.1 Effects of single faults 63
B.3.2 Influences between items 64
B.3.3 Detection of single faults 68
B.3.4 Action following detection (retention of safe state) 69
B.3.5 Effects of multiple faults 71
B.3.6 Defence against systematic faults 73
Annex C (normative) **Identification of hardware component failure modes** **74**
C.1 Introduction **74**
C.2 General procedure **74**
C.3 Procedure for integrated circuits **74**
C.4 Procedure for components with inherent physical properties **74**
C.5 General provisions concerning component failure modes **75**
Annex D (intentionally left empty) **93**
Annex E (normative) **Techniques and measures for the avoidance of systematic faults and the control of random and systematic faults** **94**
E.1 Introduction **94**
E.2 Tables of techniques and measures **96**
Annex F (informative) **Guidance on Programmable Components** **103**
F.1 Introduction **103**
F.1.1 Purpose 103
F.1.2 Objectives 103
F.1.3 Development context 104
F.1.4 Life-cycle issues and documentation 105
F.1.5 Organization, roles, responsibilities and personnel competencies 108
F.1.6 Programmable Component requirements 108
F.1.7 Programmable Component architecture and design 108
F.1.8 Logic Component design 109
F.1.9 Logic Component coding and testing 109
F.1.10 Programmable Component integration testing 109
F.1.11 Programmable Component validation 109
F.1.12 Requirements for use of pre-existing logic components 109

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

oSIST prEN 50129:2017

F.2 Detailed technical requirements for Programmable Components 109
F.2.1 Guidance on safety architecture 109
F.2.2 Protection against random faults – architectural principles 110
F.2.3 Protection against systematic faults – (techniques/measures) 110
F.2.4 Description of techniques and measures 113
Annex G (informative) Changes at this European Standard compared to EN 50129:2003 118
Annex ZZ (informative) **Relationship between this European Standard and the Essential Requirements of EU Directive 2008/57/EC 121**
Bibliography 122

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

oSIST prEN 50129:2017

European foreword

This document [prEN 50129:2016] has been prepared by CLC/SC 9XA “Communication, signalling and processing systems” of CLC/TC 9X “Electrical and electronic applications for railways”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

This document will supersede EN 50129:2003.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association, and supports essential requirements of EU Directive(s).

For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this document.

The structure is of this European standard is described in Clause 4.

Comparison of changes between EN 50129:2003 and this draft European Standard can be found in Annex G.

This draft European Standard has been prepared under the Mandate M/483 given to CENELEC by the European Commission and the Implementing Regulation (EU) No 402/2013 (with the subsequent amendment, Implementing Regulation (EU) No 2015/1136).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

oSIST prEN 50129:2017

Introduction

This European Standard should be read in conjunction with prEN 50126-1:2015, "*Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process*", prEN 50126-2:2015, "*Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety*", and EN 50128, "*Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems*".

This document defines requirements for the acceptance of safety-related electronic systems in the railway signalling field.

The aim of European railway duty holders and European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of Safety Approvals for systems, subsystems or equipment by the different national railway duty holders is necessary. This document is the common European base for safety acceptance of electronic systems for railway signalling applications.

Cross-acceptance is aimed at acceptance of generic products and generic applications, not specific applications. Public procurement within the European Community concerning safety-related electronic systems for railway signalling applications will refer to this European Standard.

This European Standard is concerned with the evidence to be presented for the acceptance of safety-related systems. However, it specifies not only those life-cycle activities which need to be completed before the acceptance stage, but also the additional planned activities to be carried out after. This way, safety justification will cover the whole life-cycle.

This European Standard is concerned with what evidence is to be presented. Except where considered appropriate, it does not specify who carries out the necessary work, since this can vary in different circumstances.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Safety-related electronic systems for signalling include hardware and software aspects. To develop complete safety-related systems, both aspects need to be taken into account throughout the whole life-cycle of the system. The requirements for the overall safety-related electronic system and for its hardware aspects are defined in this standard. Other requirements are defined in associated CENELEC standards: for safety-related systems which include software, see EN 50128; for safety-related data communication, see EN 50159.

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/150297cf-3159-4127-9c85-1a29560fa4df/sist-en-50129-2019

This European Standard consists of the main part (Clause 1 to Clause 8) and Annexes A, B, C, D, E, F, G and ZZ. The requirements defined in the main part of the standard and in Annexes A, B, C and E are normative, whilst Annexes F, G and ZZ are informative. Annex D is intentionally left empty.

In this European Standard provisions are expressed exclusively (according to “Internal Regulations Part 3: Rules for the structure and drafting of CEN-CENELEC Publications”) by means of the following verbal forms:

- “shall / shall not” for requirements;
- “should / should not” for recommendations;
- “may / need not” for permissions;
- “can / cannot” for possibilities and capabilities.

This European Standard is in line with, and uses relevant sections of:

- prEN 50126-1:2015, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process* and
- prEN 50126-2:2015, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety*.

This European standard is based on the system life-cycle described in the EN 50126 series and is in line with the EN 61508 series. The EN 50126 series/EN 50128/EN 50129 comprise the railway sector equivalent of the EN 61508 series so far as Railway Communication, Signalling and Processing Systems are concerned. When compliance with these European standards has been demonstrated, further evaluation of compliance with the EN 61508 series is not required.

oSIST prEN 50129:2017

1 Scope

This European standard is applicable to safety-related electronic systems (including subsystems and equipment) for railway signalling applications.

This European standard applies to generic systems (i.e. generic products or systems defining a class of applications), as well as to systems for specific applications.

The scope of this European standard, and its relationship with other CENELEC standards, are shown in Figure 1.

This European standard is applicable only to the functional safety of systems. It is not intended to deal with other aspects of safety such as the occupational health and safety of personnel. While functional safety of systems clearly can have an impact on the safety of personnel, there are other aspects of system design which can also affect occupational health and safety and which are not covered by this European standard.

This European standard applies to all the phases of the life-cycle of a safety-related electronic system, focusing in particular on phases from 5 (architecture and apportionment of system requirements) to 10 (system acceptance) as defined in EN 50126 (all parts).

Requirements for systems which are not related to safety are outside the scope of this European Standard.

This European standard is not applicable to existing systems, subsystems or equipment (i.e. those which had already been accepted prior to the creation of this European standard). However, as far as reasonably practicable, it should be applied to modifications and extensions to existing systems, subsystems and equipment.

This European standard is primarily applicable to systems, subsystems or equipment which have been specifically designed and manufactured for railway signalling applications. It should also be applied, as far as reasonably practicable, to general-purpose or industrial equipment (e.g. power supplies, display screens or other commercial off the shelf items), which is procured for use as part of a safety-related electronic system. As a minimum, evidence should be provided in such cases to demonstrate either

- that the equipment is not relied on for safety, or
- that the equipment can be relied on for those functions which relate to safety.

This European standard is aimed at railway duty holders, railway suppliers, and assessors as well as at safety authorities, although it does not define an approval process to be applied by the safety authorities.

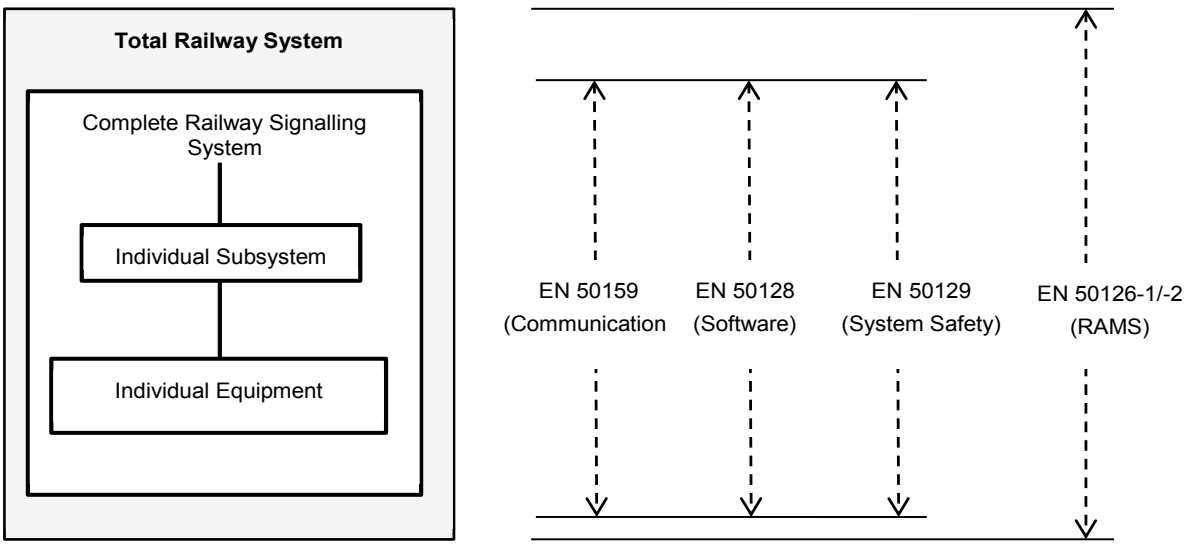

Figure 1 – Scope of the main CENELEC railway application standards

oSIST prEN 50129:2017

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

NOTE Additional informative references are included in the Bibliography.

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: Rolling stock and on-board equipment*

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

prEN 50126-1:2015, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Generic RAMS Process*

prEN 50126-2:2015, *Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to Safety*

CLC/TR 50126-3, *Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 3: Guide to the application of EN 50126-1 for rolling stock RAM*

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

EN 60664-1, *Insulation coordination for equipment within low-voltage systems - Part 1: Principles, requirements and tests (IEC 60664-1)*

EN 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures (IEC 61508-7:2010, modified)*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3 Terms, definitions and abbreviations

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

3.1 Terms and definitions

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

3.1.1
accident

unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage

[SOURCE: IEC 60050-821: CDV2015, 821-12-02]

3.1.2
availability

ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval

[SOURCE: IEC 60050-821: CDV2015, 821-05-82, modified]

3.1.3
causal analysis

analysis of the reasons how and why a particular hazard can come into existence

3.1.4
common-cause failure

failures of different items resulting from the same cause where these failures are not consequences of each other

[SOURCE: IEC 60050-821: CDV2015, 821-12-10]

oSIST prEN 50129:2017

3.1.5
configuration

structuring and interconnection of the hardware and software of a system for its intended application

[SOURCE: IEC 60050-821: CDV2015, 821-12-12]

3.1.6
consequence analysis

analysis of events which are likely to happen after a hazard has occurred

[SOURCE: IEC 60050-821: CDV2015, 821-12-14]

3.1.7
cross-acceptance

status achieved by a product that has been accepted by one authority to the relevant standards and is acceptable to other authorities without the necessity for further assessment

[SOURCE: IEC 60050-821: CDV2015, 821-12-15]

3.1.8
design

activity applied in order to analyse and transform specified requirements into acceptable solutions

[SOURCE: IEC 60050-821: CDV2015, 821-12-16, modified]

3.1.9
diversity

existence of two or more different ways or means of achieving a specified objective

Note 1 to entry: Diversity is specifically provided as a defence against common cause failure. It can be achieved by providing systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective in different ways.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: IEC 60050-395:2014, 395-07-115]

3.1.10
DC fault model

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-

fault category that includes the following failure modes: stuck-at faults, stuck-open, open or high impedance outputs as well as short circuits between signal lines, and for integrated circuits, short circuit between any two connections (pins)

[SOURCE: EN 61508-2:2010, modified]

3.1.11
electronic component

electronic device that cannot be taken apart without destruction or impairment of its intended use

Note 1 to entry: Electronic components are for instance resistors, capacitors, diodes, integrated circuits, hybrids, application specific integrated circuits, wound components and relays.

[SOURCE: IEC 62542:2013, subclause 3.3]

3.1.12
equipment

single apparatus or set of devices or apparatuses, or the set of main devices of an installation, or all devices necessary to perform a specific task

Note 1 to entry: Examples of equipment are a power transformer, the equipment of a substation, measuring equipment.

[SOURCE: IEC 60050-151:2001, 151-11-25]

3.1.13
error

discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.

Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

oSIST prEN 50129:2017

277 [SOURCE: IEC 60050-192:2015, 192-03-02]

278 **3.1.14**
279 **fail-safe**
280 able to enter or remain in a safe state in the event of a failure

281 [SOURCE: IEC 60050-821: CDV2015, 821-01-10, modified]

282 **3.1.15**
283 **failure**
284 failure (of an item) loss of ability to perform as required

285 Note 1 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

286 [SOURCE: IEC 60050-192:2015, 192-03-01]

287 **3.1.16**
288 **fault**
289 abnormal condition that could lead to an error in a system

290 Note 1 to entry: A fault can be random or systematic.

291 [SOURCE: IEC 60050-821: CDV2015, 821-11-19]

292 **3.1.17**
293 **fault detection time**
294 time interval which begins at the instant when a fault occurs and ends when the existence of the fault is
295 detected

296 [SOURCE: IEC 60050-821: CDV2015, 821-12-22]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

297 **3.1.18**
298 **function**
299 specified action or activity which can be performed by technical means and/or human beings and has a
300 defined output in response to a defined input

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

301 Note 1 to entry: A function can be specified or described without reference to the physical means of achieving it.

302 [SOURCE: IEC 60050-821: CDV2015, 821-12-25, modified]

303 **3.1.19**
304 **functional safety**
305 part of the overall safety that depends on functional and physical units operating correctly in response to
306 their inputs

307 [SOURCE: IEC 60050-351, 351-57-06]

308 **3.1.20**
309 **hardware component**
310 See 3.1.11 electronic component

311 **3.1.21**
312 **hazard**
313 condition that could lead to an accident

314 Note 1 to entry: The equivalent definition in IEC 60050-903:2013, 903-01-02 refers to "harm" that, in respect to "accident", does not
315 include loss of system or service.

316 **3.1.22**
317 **hazard analysis**
318 process of identifying hazards and analysing their causes, and the derivation of requirements to limit the
319 likelihood and consequences of hazards to a tolerable level

320 [SOURCE: IEC 60050-821: CDV2015, 821-11-22]

321 **3.1.23**
322 **hazard log**
323 document in which hazards identified, decisions made, solutions adopted and their implementation status
324 are recorded or referenced

oSIST prEN 50129:2017

[SOURCE: IEC 60050-821: CDV2015, 821-12-27]

3.1.24
implementation

activity applied in order to transform the specified designs into their realization

[SOURCE: IEC 60050-821: CDV2015, 821-12-29]

3.1.25
independence (human)

freedom from involvement in the same intellectual, commercial and/or management entity

[SOURCE: IEC 60050-821: CDV2015, 821-12-32]

3.1.26
independent safety assessment

process of analysis to determine whether the designer and the validator have achieved a product that meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety

3.1.27
maintenance

combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required

Note 1 to entry: Management is assumed to include supervision activities.

[SOURCE: IEC 60050-192:2015, 192-06-01]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.28
negation

enforcement of a safe state following detection of a hazardous fault

[SOURCE: IEC 60050-821: CDV2015, 821-12-38]

SIST EN 50129:2019
ards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-

3.1.29
negation time

time interval which begins when the existence of a fault is detected and ends when a safe state is enforced

[SOURCE: IEC 60050-821: CDV2015, 821-12-39]

3.1.30
pre-existing item

item that already exists and that was not developed specifically for the current project

3.1.31
product

collection of elements, interconnected to form a system, a subsystem or an equipment, in a manner which meets the specified requirements

[SOURCE: IEC 60050-821: CDV2015, 821-12-40]

3.1.32
railway duty holder

body with the overall accountability for operating a railway system within the legal framework

3.1.33
random failure integrity

degree to which a system is free from hazardous random faults

[SOURCE: IEC 60050-821: CDV2015, 821-12-46]

3.1.34
random fault

unpredictable occurrence of a fault

[SOURCE: IEC 60050-821: CDV2015, 821-12-47]

oSIST prEN 50129:2017

3.1.35
redundancy

(in a system) provision of more than one means for performing a function

[SOURCE: IEC 60050-192: 2015, 192-10-02]

3.1.36
reliability

(of an item) ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures.

[SOURCE: IEC 60050-192:2015, 192-01-24]

3.1.37
repair

direct action taken to effect restoration

Note 1 to entry: Repair includes fault localization (SOURCE: IEC 60050-192:2015, 192-06-19), fault diagnosis (SOURCE: IEC 60050-192:2015, 192-06-20); fault correction (SOURCE: IEC 60050-192:2015, 192-06-21); and function checkout (192).

[SOURCE: IEC 60050-192:2015, 192-06-14]

3.1.38
risk

iTeh STANDARD PREVIEW
(standards.iteh.ai)

combination of the frequency, or probability, and the consequence of a specified hazardous event

3.1.39
safe state

condition which continues to preserve safety

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

[SOURCE: IEC 60050-821: CDV2015, 821-12-50]

3.1.40
safety

freedom from unacceptable risk

SOURCE: ISO/IEC Guide 51:1999, sub-clause 3.1

[SOURCE: IEC 60050-903:2013, 903-01-19]

3.1.41
safety acceptance

safety status given to a product by the final user

[SOURCE: IEC 60050-821: CDV2015, 821-12-51]

3.1.42
safety approval

safety status given to a product by the requisite authority when the product has fulfilled a set of pre-determined conditions

[SOURCE: IEC 60050-821: CDV2015, 821-12-52]

3.1.43
safety authority

body responsible for delivering the authorization for the operation of the safety-related system

[SOURCE: IEC 60050-821: CDV2015, 821-12-53]

oSIST prEN 50129:2017

3.1.44
safety case

documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements

[SOURCE: IEC 60050-821: CDV2015, 821-12-54]

3.1.45
safety integrity

ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated duration

[SOURCE: IEC 60050-821: CDV2015, 821-12-55]

3.1.46
Safety Integrity Level

one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems

[SOURCE: EN 50126]

3.1.47
safety life-cycle

additional series of activities carried out in conjunction with the system life-cycle for safety-related systems

[SOURCE: IEC 60050-821: CDV2015, 821-12-56]

3.1.48
safety plan

iTeh STANDARD PREVIEW
(standards.iteh.ai)

documented set of time scheduled activities, resources and events serving to implement the organization, responsibilities, procedures, activities, capabilities and resources that together ensure that an item will satisfy given safety requirements relevant to a given contract or project

[SOURCE: IEC 60050-821: CDV2015, 821-12-58]

SIST EN 50129:2019
https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019

3.1.49
safety process

series of procedures that are followed to enable all safety requirements of a product to be identified and met

[SOURCE: IEC 60050-821: CDV2015, 821-12-59]

3.1.50
safety-related

carrying responsibility for safety

[SOURCE: IEC 60050-821: CDV2015, 821-01-73]

3.1.51
signalling system

system to ensure the safe movement of trains

Note 1 to entry: For the purposes of this standard, railway signalling applications encompass all systems which control and protect train movements by conveying instructions or warnings to trains or trackside systems. Where a signalling system includes subsystems or equipment on board of the train, this standard is intended to apply up to the interface with the braking system, traction control system or other relevant train systems.

[SOURCE: IEC 60050-821: CDV2015, 821-01-03, modified]

3.1.52
stress profile

degree and number of external influences which a system can withstand whilst performing its required functionality

[SOURCE: IEC 60050-821: CDV2015, 821-12-66]