

SLOVENSKI STANDARD oSIST prEN 50129:2017

01-februar-2017

Železniške naprave - Komunikacijski, signalni in procesni sistemi - Signalnovarnostni elektronski sistemi

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

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

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



iTeh Standards (https://standards.iteh.ai) Document Preview

<u>SIST EN 50129:2019</u> 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.

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.

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.

1	Conte	nts	Page
2	Europea	n foreword	5
3	Introduc	tion	6
4	1 Sco	pe	7
5	2 Norr	native references	8
6	3 Tern	ns ,definitions and abbreviations	8
7	3.1	Terms and definitions	8
8	3.2	Abbreviations	15
9	4 Ove	rall framework of this standard	16
10	5 Req	uirements for developing safety-related electronic systems	
11	5.1	Introduction	
12	5.2	The quality management process	
13	5.3	The safety management process	19
14	6 Req	uirements for elements external to the lifecycle	
15	6.1	Introduction	
16	6.2	Re-use of pre-existing items	
17	6.3	Safety-related tools for electronic systems	
18	6.4	Physical security and IT-Security	
19	7 The	Safety Case: structure and content	
20	7.1	The Safety Case structure	
21	7.2	The Technical Safety Report	
22	7.3	Different kind of Safety Cases	42
23 p	s://s7.4dar	Provisions for the Specific Application Safety Case	ist.on.50.1.20. 42 19
24	7.5	Dependencies between Safety Cases	43
25	8 Syst	em safety acceptance and subsequent phases	44
26	8.1	System safety acceptance process	44
27	8.2	Operation, maintenance and performance monitoring	47
28	8.3	Modification and retrofit	47
29	8.4	Decommissioning and disposal	47
30	Annex A	(normative) Safety Integrity Levels	48
31	A.1 Intro	oduction	48
32	A.2 Safe	ty requirements	48
33	A.3 Safe	ty integrity	49
34	A.4 Dete	rmination of safety integrity requirements	49
35	A.4.1	General	
36	A.4.2	Risk Assessment	51
37	A.4.3	Hazard Control	
38	A.4.4	Identification and treatment of new hazards arising from design	
39	A.4.5	An example of THR/TFFR/FR and SIL allocation	57

40	A.5 Assig	inment of SILS	59
41	A.5.1	General aspects	59
42	A.5.2	Relationship between SIL and associated TFFR	60
43	Annex B	(normative) Management of faults for safety-related functions	61
44	B.1 Intro	Juction	61
45	B.2 Gene	ral concepts	61
46	B.2.1	Detection and negation times	61
47	B.2.2	Composition of two independent items	62
48	B.3 Effec	ts of faults	63
49	B.3.1	Effects of single faults	63
50	B.3.2	Influences between items	64
51	B.3.3	Detection of single faults	68
52	B.3.4	Action following detection (retention of safe state)	69
53	B.3.5	Effects of multiple faults	71
54	B.3.6	Defence against systematic faults	73
55	Annex C	(normative) Identification of hardware component failure modes	74
56	C.1 Intro	Juction	74
57	C.2 Gene	ral procedure	74
58	C.3 Proc	edure for integrated circuits	74
59	C.4 Proc	edure for components with inherent physical properties	74
60	C.5 Gene	ral provisions concerning component failure modes	75
61	Annex D	(intentionally left empty)	93
62 63 ps	Annex E	normative) Techniques and measures for the avoidance of systematic faults a	
	001111010	random and systematic faults	ind the
64	E.1 Intro	random and systematic faults	ind the
64 65	E.1 Intro	random and systematic faults	and the
64 65 66	E.1 Intro E.2 Table Annex F (random and systematic faults duction s of techniques and measures informative) Guidance on Programmable Components	and the 94
64 65 66 67	E.1 Intro E.2 Table Annex F (F.1 Intro	random and systematic faults <u>Second Representation</u> duction <u>second</u> so of techniques and measures <u>second</u> so of techniques and measures <u>second</u> second s	and the 94
64 65 66 67 68	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1	random and systematic faults	10 the
64 65 66 67 68 69	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2	random and systematic faults	
64 65 66 67 68 69 70	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3	random and systematic faults duction s of techniques and measures informative) Guidance on Programmable Components Juction Purpose Objectives Development context	103
64 65 66 67 68 69 70 71	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4	f random and systematic faults	
64 65 66 67 68 69 70 71 72	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5	random and systematic faults duction s of techniques and measures informative) Guidance on Programmable Components duction duction Purpose Objectives Development context Life-cycle issues and documentation Organization, roles, responsibilities and personnel competencies	
64 65 67 68 69 70 71 72 73	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6	f random and systematic faults	
64 65 67 68 69 70 71 72 73 74	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6 F.1.7	f random and systematic faults	ind the
64 65 67 68 69 70 71 72 73 74 75	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6 F.1.7 F.1.8	random and systematic faults	ind the
64 65 66 67 68 69 70 71 72 73 74 75 76	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6 F.1.7 F.1.8 F.1.9	random and systematic faults	ind the
64 65 66 67 68 69 70 71 72 73 74 75 76 77	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6 F.1.7 F.1.8 F.1.9 F.1.10	random and systematic faults	ind the
 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 	E.1 Intro E.2 Table Annex F (F.1 Intro F.1.1 F.1.2 F.1.3 F.1.4 F.1.5 F.1.6 F.1.7 F.1.8 F.1.9 F.1.10 F.1.11	random and systematic faults	ind the

oSIST prEN 50129:2017

prEN 50129:2016

80	F.2 Deta	iled technical requirements for Programmable Components	109
81	F.2.1	Guidance on safety architecture	109
82	F.2.2	Protection against random faults – architectural principles	110
83	F.2.3	Protection against systematic faults – (techniques/measures)	110
84	F.2.4	Description of techniques and measures	113
85	Annex G	(informative) Changes at this European Standard compared to EN 50129:2003	118
86 87	Annex Z Requirer	Z (informative) Relationship between this European Standard and the Essential nents of EU Directive 2008/57/EC	121
88	Bibliogra	iphy	122
89			

iTeh Standards (https://standards.iteh.ai) Document Preview

SIST EN 50129:2019

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

90 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".
- 93 This document is currently submitted to the Enquiry.
- 94 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)

- 95 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).
- 98 For the relationship with EU Directive(s) see informative Annex ZZ, which is an integral part of this 99 document.
- 100 The structure is of this European standard is described in Clause 4.
- 101 Comparison of changes between EN 50129:2003 and this draft European Standard can be found in 102 Annex G.
- 103 This draft European Standard has been prepared under the Mandate M/483 given to CENELEC by the
- 104 European Commission and the Implementing Regulation (EU) No 402/2013 (with the subsequent
- amendment, Implementing Regulation (EU) No 2015/1136).

SIST EN 50129:2019

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

106 Introduction

107 This European Standard should be read in conjunction with prEN 50126-1:2015, "Railway Applications —

108The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) —109Part 1: Generic RAMS Process", prEN 50126-2:2015, "Railway Applications — The Specification and100Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 2: Systems Approach to111Safety", and EN 50128, "Railway applications — Communication, signalling and processing systems —

112 Software for railway control and protection systems".

113 This document defines requirements for the acceptance of safety-related electronic systems in the railway 114 signalling field.

115 The aim of European railway duty holders and European railway industry is to develop compatible railway 116 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

118 common European base for safety acceptance of electronic systems for railway signalling applications.

119 Cross-acceptance is aimed at acceptance of generic products and generic applications, not specific 120 applications. Public procurement within the European Community concerning safety-related electronic 121 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 safetyrelated 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.

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,

134 see EN 50159.

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:

- 141 "shall / shall not" for requirements;
- 142 "should / should not" for recommendations;
- 143 "may / need not" for permissions;
- 144 "can / cannot" for possibilities and capabilities.
- 145 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.

155 **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.

160 The scope of this European standard, and its relationship with other CENELEC standards, are shown in 161 Figure 1.

162 This European standard is applicable only to the functional safety of systems. It is not intended to deal with 163 other aspects of safety such as the occupational health and safety of personnel. While functional safety of 164 systems clearly can have an impact on the safety of personnel, there are other aspects of system design 165 which can also affect occupational health and safety and which are not covered by this European standard.

166 This European standard applies to all the phases of the life-cycle of a safety-related electronic system, 167 focusing in particular on phases from 5 (architecture and apportionment of system requirements) to 10 168 (system acceptance) as defined in EN 50126 (all parts).

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

170 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

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

181 This European standard is aimed at railway duty holders, railway suppliers, and assessors as well as at 182 safety authorities, although it does not define an approval process to be applied by the safety authorities.

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



183 184

Figure 1 – Scope of the main CENELEC railway application standards

185 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.

- 189 NOTE Additional informative references are included in the Bibliography.
- 190 EN 50124-1, *Railway applications Insulation coordination Part 1: Basic requirements Clearances and* 191 creepage distances for all electrical and electronic equipment
- 192 EN 50125-1, Railway applications Environmental conditions for equipment Part 1: Rolling stock and 193 on-board equipment
- 194 EN 50125-3, Railway applications Environmental conditions for equipment Part 3: Equipment for 195 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)

208 **3 Terms, definitions and abbreviations**

209 3.1 Terms and definitions SIST EN 50129:2019

https://standards.iteh.ai/catalog/standards/sist/f50297ef-3f39-4f27-9e85-1a295b0fa4df/sist-en-50129-2019 210 For the purposes of this document, the following terms and definitions apply.

- 211 **3.1.1**
- 212 accident

213 unintended event or series of events that results in death, injury, loss of a system or service, or 214 environmental damage

- 215 [SOURCE: IEC 60050-821: CDV2015, 821-12-02]
- 216 **3.1.2**

217 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

- 220 [SOURCE: IEC 60050-821: CDV2015, 821-05-82, modified]
- 221 **3.1.3**

222 causal analysis

- analysis of the reasons how and why a particular hazard can come into existence
- 224 **3.1.4**

225 common-cause failure

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

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

3.1.5 229 230 configuration structuring and interconnection of the hardware and software of a system for its intended application 231 [SOURCE: IEC 60050-821: CDV2015, 821-12-12] 232 3.1.6 233 234 consequence analysis 235 analysis of events which are likely to happen after a hazard has occurred 236 [SOURCE: IEC 60050-821: CDV2015, 821-12-14] 3.1.7 237 238 cross-acceptance status achieved by a product that has been accepted by one authority to the relevant standards and is 239 240 acceptable to other authorities without the necessity for further assessment [SOURCE: IEC 60050-821: CDV2015, 821-12-15] 241 3.1.8 242 243 design activity applied in order to analyse and transform specified requirements into acceptable solutions 244 245 [SOURCE: IEC 60050-821: CDV2015, 821-12-16, modified] 3.1.9 246 247 diversity 248 existence of two or more different ways or means of achieving a specified objective 249 Note 1 to entry: Diversity is specifically provided as a defence against common cause failure. It can be achieved by providing 250 systems that are physically different from each other or by functional diversity, where similar systems achieve the specified objective 251 in different ways. [SOURCE: IEC 60050-395:2014, 395-07-115] 252 **Document Preview** 3.1.10 253 DC fault model 254

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)

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

259 **3.1.11**

260 electronic component

261 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.

- 264 [SOURCE: IEC 62542:2013, subclause 3.3]
- 265 **3.1.12**

266 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

- 269 Note 1 to entry: Examples of equipment are a power transformer, the equipment of a substation, measuring equipment.
- 270 [SOURCE: IEC 60050-151:2001, 151-11-25]

271 **3.1.13**

272 **error**

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

- 275 Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.
- 276 Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.

prEN 50129:2016

- 277 [SOURCE: IEC 60050-192:2015, 192-03-02]
- 278 **3.1.14**
- 279 fail-safe
- 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
- 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
- time interval which begins at the instant when a fault occurs and ends when the existence of the fault is detected
- 296 [SOURCE: IEC 60050-821: CDV2015, 821-12-22]
- 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
- 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 3.1.19 3.1.19**
- 303 5.1.19 304 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
- 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 include loss of system or service.
- 316 **3.1.22**
- 317 hazard analysis
- process of identifying hazards and analysing their causes, and the derivation of requirements to limit the 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
- document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced

prEN 50129:2016

325	[SOURCE: IEC 60050-821: CDV2015, 821-12-27]
326	3.1.24
327	implementation
328	
329	[SOURCE: IEC 60050-821: CDV2015, 821-12-29]
330 331	3.1.25 independence (human)
332	freedom from involvement in the same intellectual, commercial and/or management entity
333	[SOURCE: IEC 60050-821: CDV2015, 821-12-32]
334 335	3.1.26 independent safety assessment
336 337 338	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
339	3.1.27
340	maintenance
342	which it can perform as required
343	Note 1 to entry: Management is assumed to include supervision activities.
344	[SOURCE: IEC 60050-192:2015, 192-06-01]
345 346	3.1.28 ileh Standards
347	enforcement of a safe state following detection of a hazardous fault
348	[SOURCE: IEC 60050-821: CDV2015, 821-12-38]
349 350	3.1.29 DOCUMENT Preview
351	time interval which begins when the existence of a fault is detected and ends when a safe state is enforced
352 08	[SOURCE: IEC 60050-821: CDV2015, 821-12-39]7ef-3/39-4/27-9e85-1a295b0fa4df/sist-en-50129-2019
353	3.1.30
354	pre-existing item
355	item that already exists and that was not developed specifically for the current project
356 357	3.1.31 product
358	collection of elements, interconnected to form a system, a subsystem or an equipment, in a manner which
359	meets the specified requirements
360	[SOURCE: IEC 60050-821: CDV2015, 821-12-40]
361	3.1.32
362	railway duty noider
364	3 1 33
365	random failure integrity
366	degree to which a system is free from hazardous random faults
367	[SOURCE: IEC 60050-821: CDV2015, 821-12-46]
368	3.1.34
369	random fault
370	
3/1	[300K0E. IEC 00030-021. CDV2013, 021-12-47]

prEN 50129:2016

372 373	3.1.35 redundancy
374	(in a system) provision of more than one means for performing a function
375	[SOURCE: IEC 60050-192: 2015, 192-10-02]
376 377	3.1.36 reliability
378	(of an item) ability to perform as required, without failure, for a given time interval, under given conditions
379 380	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.
381 382	Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.
383	Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, Reliability related concepts: measures.
384	[SOURCE: IEC 60050-192:2015, 192-01-24]
385 386	3.1.37 repair
387	direct action taken to effect restoration
388 389	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).
390	[SOURCE: IEC 60050-192:2015, 192-06-14]
391 302	3.1.38 risk
393	combination of the frequency, or probability, and the consequence of a specified hazardous event
394 395	3.1.39 (https://standards.iteh.ai)
396	condition which continues to preserve safety
397	[SOURCE: IEC 60050-821: CDV2015, 821-12-50]
398	3.1.40 <u>SIST EN 50129:2019</u>
399 400	safety freedom from unacceptable risk
401	SOURCE: ISO/IEC Guide 51:1999, sub-clause 3.1
402	[SOURCE: IEC 60050-903:2013, 903-01-19]
403	3.1.41
404	safety acceptance
405	Salety status given to a product by the final user $[SOLIPCE \cdot IEC 60050 821 \cdot CDV2015, 821, 12, 51]$
400	3 1 <i>1</i> 2
408	safety approval
409 410	safety status given to a product by the requisite authority when the product has fulfilled a set of pre- determined conditions
411	[SOURCE: IEC 60050-821: CDV2015, 821-12-52]
412	3.1.43
413	safety authority
414	
415	[300KGE. IEG 00030-021: GDV2013, 021-12-33]