



SLOVENSKI STANDARD
oSIST prEN 50126-1:2013
01-januar-2013

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 1. del: Generični procesi RAMS

Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 1: Generischer RAMS- Prozess

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 1: Processus FDMS générique

<https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pr-en-50126-1-2012>

Ta slovenski standard je istoveten z: prEN 50126-1:2012

ICS:

29.280	Električna vlečna oprema	Electric traction equipment
45.020	Železniška tehnika na splošno	Railway engineering in general

oSIST prEN 50126-1:2013

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[oSIST prEN 50126-1:2012](https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012>

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 50126-1

October 2012

ICS 45.020

Will supersede EN 50126-1:1999 (partially), CLC/TR 50126-2:2007, CLC/TR 50126-3:2008

English version

**Railway applications -
The Specification and Demonstration of Reliability, Availability,
Maintainability and Safety (RAMS) -
Part 1: Generic RAMS process**

Applications ferroviaires -
Spécification et démonstration de la fiabilité,
de la disponibilité, de la maintenabilité et de
la sécurité (FDMS) -
Partie 1: Processus FDMS générique

Bahnanwendungen -
Spezifikation und Nachweis von
Zuverlässigkeit, Verfügbarkeit,
Instandhaltbarkeit und Sicherheit (RAMS) -
Teil 1: Generischer RAMS- Prozess

iTeh STANDARD PREVIEW

This draft European Standard is submitted to CENELEC members for CENELEC enquiry.
Deadline for CENELEC: 2013-03-29 (standards.iteh.ai)

It has been drawn up by CLC/TC 9X.

oSIST prEN 50126-1:2012

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.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

1	Contents	Page
2	Foreword	6
3	Introduction	7
4	1 Scope	9
5	2 Normative references	10
6	3 Terms and definitions	10
7	4 Abbreviations	19
8	5 Process overview	20
9	5.1 Purpose of overview	20
10	5.2 Objective	20
11	5.3 Management responsibility	20
12	5.4 Adaptability to project scope and size	20
13	5.5 Interrelation of RAMS management process and life-cycle	21
14	5.6 Short description of life-cycle phases	23
15	6 Railway RAMS	24
16	6.1 Introduction	24
17	6.2 System-level approach	24
18	6.2.1 Concepts of system hierarchy	24
19	6.2.2 A system's requirements and characteristics	25
20	6.2.3 Defining a system	26
21	6.3 Railway system overview	26
22	6.3.1 Introduction	26
23	6.3.2 Bodies/entities involved in a railway system	27
24	6.3.3 Railway system environment and the balance of requirements	27
25	6.3.4 Railway system structure and apportionment of RAMS requirements	27
26	6.4 Railway RAMS and quality of service	28
27	6.5 Elements of railway RAMS	28
28	6.6 Factors influencing railway RAMS	29
29	6.6.1 General	29
30	6.6.2 Classes of failures	30
31	6.6.3 Derivation of detailed railway specific influencing factors	30
32	6.6.4 Evaluation of factors	34
33	6.7 Specification of railway RAMS requirements	34
34	6.7.1 General	34
35	6.7.2 RAMS specification	34
36	6.8 Risk based approach	35
37	6.9 Risk reduction strategy	36
38	6.9.1 Introduction	36
39	6.9.2 Reduction of risks related to safety	36
40	6.10 Safety integrity	37
41	6.10.1 Safety integrity concept	37
42	7 Management of railway RAMS	38
43	7.1 RAMS process	38

44	7.1.1	General	38
45	7.1.2	Safety management within the RAMS Process	38
46	7.1.3	Independence of roles	39
47	7.2	System life-cycle	39
48	7.3	Application and tailoring of this standard	46
49	7.4	General requirements on RAMS documentation	47
50	8	RAMS life-cycle	48
51	8.1	General	48
52	8.2	Phase 1: concept	48
53	8.2.1	Objectives	48
54	8.2.2	Activities	48
55	8.2.3	Deliverables	49
56	8.2.4	Specific verification tasks	49
57	8.2.5	Specific validation tasks	49
58	8.3	Phase 2: system definition and operational context	49
59	8.3.1	Objectives	49
60	8.3.2	Activities	49
61	8.3.3	Deliverables	53
62	8.3.4	Specific verification tasks	53
63	8.3.5	Specific validation tasks	53
64	8.4	Phase 3: risk analysis and evaluation	53
65	8.4.1	Objectives	53
66	8.4.2	Activities	54
67	8.4.3	Deliverables	55
68	8.4.4	Specific verification tasks	55
69	8.4.5	Specific validation tasks	55
70	8.5	Phase 4: specification of system requirements	56
71	8.5.1	Objectives	56
72	8.5.2	Activities	56
73	8.5.3	Deliverables	57
74	8.5.4	Specific verification tasks	57
75	8.5.5	Specific validation tasks	57
76	8.6	Phase 5: architecture and apportionment of system requirements	57
77	8.6.1	Objectives	57
78	8.6.2	Activities	58
79	8.6.3	Deliverables	58
80	8.6.4	Specific verification tasks	59
81	8.6.5	Specific validation tasks	59
82	8.7	Phase 6: design and implementation	59
83	8.7.1	Objectives	59
84	8.7.2	Activities	59
85	8.7.3	Deliverables	60
86	8.7.4	Specific verification tasks	60
87	8.7.5	Specific validation tasks	60
88	8.8	Phase 7: manufacture	60
89	8.8.1	Objectives	60
90	8.8.2	Activities	60
91	8.8.3	Deliverables	61
92	8.8.4	Specific verification tasks	61

93	8.8.5	Specific validation tasks.....	61
94	8.9	Phase 8: integration.....	61
95	8.9.1	Objectives.....	61
96	8.9.2	Activities.....	61
97	8.9.3	Deliverables.....	62
98	8.9.4	Specific verification tasks.....	62
99	8.9.5	Specific validation tasks.....	62
100	8.10	Phase 9: system validation.....	62
101	8.10.1	Objectives.....	62
102	8.10.2	Activities.....	62
103	8.10.3	Deliverables.....	63
104	8.10.4	Specific verification tasks.....	63
105	8.10.5	Specific validation tasks.....	63
106	8.11	Phase 10: system acceptance.....	63
107	8.11.1	Objectives.....	63
108	8.11.2	Activities.....	63
109	8.11.3	Deliverables.....	64
110	8.11.4	Specific verification tasks.....	64
111	8.11.5	Specific validation tasks.....	64
112	8.12	Phase 11: operation, maintenance and performance monitoring.....	64
113	8.12.1	Objectives.....	64
114	8.12.2	Activities.....	64
115	8.12.3	Deliverables.....	65
116	8.12.4	Specific verification tasks.....	65
117	8.12.5	Specific validation tasks.....	65
118	8.13	Phase 12: decommissioning.....	65
119	8.13.1	Objectives.....	65
120	8.13.2	Activities.....	66
121	8.13.3	Deliverables.....	66
122	8.13.4	Specific verification tasks.....	66
123	8.13.5	Specific validation tasks.....	66
124	9	Risk assessment.....	66
125	9.1	Scope.....	66
126	9.2	Risk analysis methodology.....	66
127	9.3	Risk evaluation and acceptance.....	69
128	9.3.1	Acceptance principles.....	69
129	9.3.2	Methods for determining risk acceptance criteria.....	69
130	10	Deliverables and structure of a safety case.....	70
131	10.1	Purpose of a safety case.....	70
132	10.2	Types of safety case.....	70
133	10.3	Safety case structure.....	71
134	10.3.1	General.....	71
135	10.3.2	Definition of system.....	72
136	10.3.3	Quality management report.....	73
137	10.3.4	Safety management report.....	73
138	10.3.5	Technical safety report.....	74
139	10.3.6	Related safety cases.....	75
140	10.3.7	Conclusion.....	75
141	10.3.8	References.....	75

142	Annex A (informative) RAMS plan	76
143	Annex B (informative) Examples of parameters for railway	81
144	B.1 Reliability parameters	81
145	B.2 Maintainability parameters	81
146	B.3 Availability parameters	82
147	B.4 Logistic support parameters	83
148	B.5 Safety parameters	84
149	Annex C (informative) Hazards at railway system level – example structured list.....	85
150	C.1 Example list	86
151	Annex D (informative) Risk matrix calibration and risk acceptance categories	91
152	D.1 Frequency of occurrence levels	91
153	D.2 Severity levels	92
154	D.3 Risk acceptance categories	93
155	Bibliography	95
156		
157	Figure 1 – Interrelation of RAMS-management process and system life-cycle	22
158	Figure 2 – Illustration of system hierarchy	25
159	Figure 3 – Example of deriving cause/effect relations in a diagrammatic approach.....	32
160	Figure 4 – Relationship of cause, hazard and accident.....	36
161	Figure 5 – The "V" representation drawing	41
162	Figure 6 – Verification	42
163	Figure 7 – Validation	42
164	Figure 8 – Structure of a safety case.....	72
165	Figure B.1 – Availability concept and related terms	83
166		
167	Table 1 – System phase related tasks (informative)	43
168	Table 2 – Frequency – Severity matrix	69
169	Table A.1 – Example of a basic RAMS plan outline	77
170	Table B.1 – Examples of reliability parameters	81
171	Table B.2 – Examples of maintainability parameters	81
172	Table B.3 – Examples of availability parameters	82
173	Table B.4 – Examples of logistic support parameters	83
174	Table B.5 – Examples of safety performance parameters	84
175	Table C.1 – Example for a hazard list.....	87
176	Table C.2 – Example scenarios.....	89
177	Table D.1 – Frequency of occurrence of events with examples for quantification (time based) ..	91
178	Table D.2 – Frequency of occurrence of events with examples for quantification (distance based)	92
179	Table D.3 – Severity categories (example related to RAM).....	92
180	Table D.4 – Severity categories (example 1 related to RAMS).....	93
181	Table D.5 – Categories (example 2 related to Safety)	93
182	Table D.6 – Financial severity levels (example).....	93
183	Table D.7 – Risk acceptance categories (example 1 for binary decisions)	93
184	Table D.8 – Risk acceptance categories (example 2)	94
185	Table D.9 – Risk acceptance categories (example related to safety)	94
186		

187 **Foreword**

188 This document [prEN 50126-1:2012] has been prepared by CLC/TC 9X "Electrical and electronic
189 applications for railways".

190 This document is currently submitted to the Enquiry.

191 EN 50126 "*Railway applications – The specification and demonstration of Reliability, Availability,
192 Maintainability and Safety (RAMS)*" consists of the following parts:

193 – Part 1: Generic RAMS process;

194 – Part 2: Systems approach to safety;

195 – Part 4: Functional safety – Electrical/Electronic/Programmable electronic systems;

196 – Part 5: Functional safety – Software.

197 This new edition of EN 50126 (all parts) will supersede EN 50126-1:1999,
198 CLC/TR 50126-2:2007, CLC/TR 50126-3:2008, EN 50128:2011 and EN 50129:2003.

199 This part of EN 50126 covers the RAMS process. It is mainly based on EN 50126-1:1999.

200 This part of EN 50126 will supersede EN 50126-1:1999 (together with prEN 50126-2:2012),
201 CLC/TR 50126-2:2007 and CLC/TR 50126-3:2008.

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

(standards.iteh.ai)

[oSIST prEN 50126-1:2012](https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012)

[https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-
2597c9c269bd/osist-pren-50126-1-2012](https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012)

205 Introduction

206 EN 50126-1:1999 was produced to introduce the application of a systematic RAMS management
207 process in the railway sector. For safety-related electronic systems for signalling, EN 50128 and
208 EN 50129 were produced. Through the application of these standards and the experiences
209 gained over the last years, the need for revision and restructuring became apparent with a need
210 to deliver a systematic and coherent approach to RAMS applicable to all the railway application
211 fields Signalling, Rolling Stock and Electric power supply for Railways (Fixed Installations).

212 The revision work improved the coherency and consistency of the standards, the concept of
213 safety management and the practical usage of EN 50126 and took into consideration the existing
214 and related Technical Reports as well.

215 This European Standard provides railway duty holders and the railway suppliers, throughout the
216 European Union, with a process which will enable the implementation of a consistent approach to
217 the management of reliability, availability, maintainability and safety, denoted by the acronym
218 RAMS.

219 Processes for the specification and demonstration of RAMS requirements are cornerstones of
220 this standard. This European Standard promotes a common understanding and approach to the
221 management of RAMS.

222 EN 50126 is the railway sector specific application of IEC 61508. Meeting the requirements in
223 this European Standard is sufficient to ensure that additional compliance to IEC 61508 does not
224 need to be demonstrated.

225 With regard to safety EN 50126-1 provides a Safety Management Process which is supported by
226 guidance and methods described in EN 50126-2.

227 EN 50126-1 and EN 50126-2 are independent from the technology used. EN 50126-4 and
228 EN 50126-5 provide guidance specific to safety-related E/E/PE technology of railway
229 applications. Their application is determined through the application of the general RAMS
230 process of EN 50126-1 and through the outcome of the safety-related methods described in
231 EN 50126-2. As far as safety is concerned, EN 50126 takes the perspective of functional safety.
232 This does not exclude other aspects of safety. However, these are not the focus.

233 The aims set for revision of EN 50126 required a better understanding of the systems approach
234 and improved methods for applying the safety management process described in EN 50126-1.
235 EN 50126-2 provides this guidance.

236 The application of this standard should be adapted to the specific requirements of the system
237 under consideration.

238 This European Standard can be applied systematically by the railway duty holders and railway
239 suppliers, throughout all phases of the life-cycle of a railway application, to develop railway
240 specific RAMS requirements and to achieve compliance with these requirements. The systems-
241 level approach developed by this European Standard facilitates assessment of the RAMS
242 interactions between elements of railway applications even if they are of complex nature.

243 This European Standard promotes co-operation between the stakeholders of Railways in the
244 achievement of an optimal combination of RAMS and cost for railway applications. Adoption of
245 this European Standard will support the principles of the European Single Market and facilitate
246 European railway inter-operability.

247 The process defined by this European Standard assumes that railway duty holders and railway
248 suppliers have business-level policies addressing Quality, Performance and Safety. The
249 approach defined in this standard is consistent with the application of quality management
250 requirements contained within the ISO 9001.

251 In accordance with CENELEC editing rules ¹⁾, mandatory requirements in this standard are
252 indicated with the modal verb “shall”. Where justifiable, the standard permits process tailoring.
253 Specific guidance on the application of this standard in the case of process tailoring is provided
254 in 7.3 of EN 50126-1. EN 50126-2 provides various methods for use in the safety management
255 process. Where a particular method is selected for the system under consideration, the
256 mandatory requirements of this method are by consequence mandatory for the safety
257 management of the system under consideration.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[oSIST prEN 50126-1:2012](https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012)

<https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012>

1) CENELEC “Internal Regulations Part 3: Rules for the structure and drafting of CEN/CENELEC Publications (2009-08), Annex H

258 1 Scope

259 This part 1 of EN 50126

- 260 • considers RAMS, understood as reliability, availability, maintainability and safety and their
261 interaction;
- 262 • considers the generic aspects of the RAMS life-cycle. The guidance in this part is still
263 applicable in the application of specific standards;
- 264 • defines
 - 265 – a process, based on the system life-cycle and tasks within it, for managing RAMS;
 - 266 – a systematic process, tailorable to the type and size of system under consideration, for
267 specifying requirements for RAMS and demonstrating that these requirements are
268 achieved;
- 269 • addresses railway specifics;
- 270 • enables conflicts between RAMS elements to be controlled and managed effectively;
- 271 • does not define
 - 272 – RAMS targets, quantities, requirements or solutions for specific railway applications;
 - 273 – rules or processes pertaining to the certification of railway products against the
274 requirements of this standard;
 - 275 – an approval process by the safety authority;
- 276 • does not specify requirements for ensuring system security.

277 This part 1 of EN 50126 is applicable

- 278 • to the specification and demonstration of RAMS for all railway applications and at all levels
279 of such an application, as appropriate, from complete railway systems to major systems and
280 to individual and combined sub-systems and components within these major systems,
281 including those containing software, in particular:
 - 282 – to new systems;
 - 283 – to new systems integrated into existing systems in operation prior to the creation of this
284 standard, although it is not generally applicable to other aspects of the existing system;
 - 285 – to modifications of existing systems in operation prior to the creation of this standard,
286 although it is not generally applicable to other aspects of the existing system;
- 287 • at all relevant phases of the life-cycle of an application;
- 288 • for use by railway duty holders and the railway suppliers.

289 It is not required to apply this standard to existing systems including those systems already
290 compliant with any version of former EN 50126, EN 50128 or EN 50129, which remain
291 unmodified. Railway applications mean Command, Control & Signalling, Rolling Stock and
292 Electric Power Supply for Railways (Fixed Installations).

293 In this standard the term hardware refers to E/E/PE components or systems. If non E/E/PE
294 hardware is meant, this is specifically mentioned.

295 2 Normative references

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

300 ISO 9001, Quality management systems – Requirements

301 ISO/IEC GUIDE 51, Safety aspects – Guidelines for their inclusion in standards

302 3 Terms and definitions

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

304 3.1

305 acceptance

306 the status achieved by a product, system or process once it has been agreed that it is suitable
 307 for its intended purpose

308 3.2

309 accident

310 an unintended event or series of events resulting in loss of human health or life, damage to
 311 property or environmental damage

312 Note 1 to entry: The term includes losses from accidents arising within a short time scale (e.g. collision, explosion)
 313 and also those incurred over the long-term (e.g. release of a toxic substance).

314 3.3

315 application conditions

316 those conditions which need to be met in order for a system to be safely integrated and safely
 317 operated.

318 Note 1 to entry: Application conditions can for example be: operational restrictions (e.g. speed limit, maximum
 319 duration of use) operational rules, maintenance restrictions (e.g. requested maintenance intervals) or environmental
 320 conditions.

321 3.4

322 approval

323 the legal act, often focused on safety, to allow a product, system or process to be placed into
 324 service

325 Note 1 to entry: A legal act can be performed by an authorised entity (i.e. a NOBO)

326 3.5

327 assessment

328 process to form a judgement on whether a product, system or process meets the specified
 329 requirements, based on evidence

330 Note 1 to entry: Independence of assessment is only necessary where explicitly specified.

331 3.6

332 assessor

333 an entity that carries out an assessment

334 Note 1 to entry: Independence of the assessor is only necessary where explicitly specified.

335 3.7

336 assurance

337 confidence in achieving a goal being pursued. Declaration intended to give confidence

338 3.8

339 audit

340 a documented, systematic and independent examination to determine whether the procedures
 341 specific to the requirements

- 342 • comply with the planned arrangements,
- 343 • are implemented effectively and
- 344 • are suitable to achieve the specified objectives

345 **3.9**346 **availability**

347 the ability of a product to be in a state to perform a required function under given conditions at a
 348 given instant of time or over a given time interval assuming that the required external resources
 349 are provided

350 Note 1 to entry: Figure B.1 (Annex B) illustrates the concept of availability and clarifies the correct use of contributory
 351 terms.

352 **3.10**353 **collective risk**

354 a risk, resulting from e.g. a product, process or system, to which a population or group of people
 355 is exposed

356 Note 1 to entry: Collective risk is not to be confused with multiple victim accidents.

357 Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group.
 358 However, the collective risk divided by the number of individuals will only provide the average individual risk.

359 Note 3 to entry: A group of people could be, for example, rail staff working in a restaurant car or all passengers using
 360 a particular network.

361 **3.11**362 **commercial off-the-shelf software**

363 software defined by market-driven need, commercially available and whose fitness for purpose
 364 has been deemed acceptable by a broad spectrum of commercial users

365 **3.12**366 **common cause failure**

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

369 **3.13**370 **compliance**

371 a state where a characteristic or property of a product, system or process satisfies the specified
 372 requirements

373 **3.14**374 **configuration management**

375 a discipline applying technical and administrative direction and surveillance to identify and
 376 document the functional and physical characteristics of a configuration item, to control changes
 377 to those characteristics, to record and report change processing and implementation status and
 378 to verify compliance with specified requirements

379 **3.15**380 **consequence analysis**

381 to analyze the consequences of each hazard up to accidents and losses

382 **3.16**383 **corrective maintenance**

384 the maintenance carried out after fault recognition and intended to put a product into a state in
 385 which it can perform a required function

386 **3.17**387 **data-driven software**

388 software configured by data and/or algorithms for producing the executable software for an
 389 application by making use of an existing generic software

390 **3.18**391 **designer**

392 an entity that analyses and transforms specified requirements into acceptable design solutions
 393 which have the required safety integrity

394 **3.19**395 **deterministic**

396 expresses that a behaviour can be predicted with certainty

397 Note 1 to entry: A deterministic event in a system can be predicted with certainty from preceding events which are
 398 either known or are the same as for a proven equivalent system.

399 **3.20**400 **diversity**

iTeh STANDARD PREVIEW
 (standards.iteh.ai)

oSIST prEN 50126-1:2012

http://standards.iteh.ai/catalog/standards/sist/87f44949-87f4-4949-87f4-4949/sist-50126-1-2012

401 a means of achieving all or part of the specified requirements in more than one independent and
402 dissimilar manner

403 Note 1 to entry: Diversity may be achieved by different physical methods or different design approaches.

404 **3.21**

405 **entity**

406 a person, group or organisation who fulfil a role as defined in this standard

407 **3.22**

408 **equivalent fatality**

409 an expression of fatalities and weighted injuries and a convention for combining injuries and
410 fatalities into one figure for ease of evaluation and comparison of risks

411 **3.23**

412 **error**

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

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

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

417 **3.24**

418 **fail-safe**

419 a concept which is incorporated into the design of a product such that, in the event of a failure, it
420 enters or remains in a safe state

421 **3.25**

422 **failure**

423 the termination of the ability of an item to perform a required function

424 Note 1 to entry: After failure the item has a fault.

425 Note 2 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

426 **3.26**

427 **failure mode**

428 a predicted or observed manner in which the product, system or process under consideration can
429 fail

<https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012>

430 **3.27**

431 **failure rate**

432 the limit, if this exists, of the ratio of the conditional probability that the instant of time, T , of a
433 failure of a product falls within a given time interval $(t, t+\Delta t)$ and the length of this interval, Δt ,
434 when Δt tends towards zero, given that the item is in an up state at the start of the time interval

435 Note 1 to entry: Failure rates are often assumed as constant. This is not always valid, e.g. for components subject to
436 wear out (mechanical, pneumatic, electromechanical, etc.).

437 **3.28**

438 **fault**

439 the state of an item characterized by inability to perform a required function, excluding the
440 inability during preventive maintenance or other planned actions

441 Note 1 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure (e.g. in case
442 of a design fault).

443 **3.29**

444 **fault detection time**

445 time span which begins at the instant when a failure occurs and ends when the existence of the
446 fault is detected

447 **3.30**

448 **fault tolerance**

449 ability of a functional unit to continue to perform a required function in the presence of faults or
450 errors

451 **3.31**

452 **firmware**

453 an ordered set of instructions and associated data stored in a way that is functionally
454 independent of main storage

3.32**function**

a specified action or activity which may be performed by technical means and/or human beings and has a defined output in response to a defined input

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

3.33**functional safety**

the perspective of safety focused on the functions of a system

Note 1 to entry: Functional safety does not only consider normal operation.

Note 2 to entry: Functional safety can be based on safety functions as well as on safety-related functions.

3.34**generic product**

product (hardware and/or software) which can be used for a variety of installations, either without making any changes or purely through the configuration of the hardware or the software (for example by the provision of application-specific data and/or algorithms)

3.35**hazard**

a condition that could lead to an accident

3.36**hazard analysis**

an analysis comprising hazard identification, causal analysis and common cause analysis

3.37**hazard log**

the document in which hazards identified, decisions made, solutions adopted and their implementation status are recorded or referenced

Note 1 to entry: The Hazard Log compiles evidence on the implementation of safety requirements regarding all identified hazards, thus supporting the demonstration of completeness of the safety assurance activities

Note 2 to entry: A "hazard record" is an extract of the hazard log that is suitable for transferring between stakeholders.

[oSIST prEN 50126-1:2012](https://standards.iteh.ai/catalog/standards/sist/94af8006-8472-43c9-b389-2597c9c269bd/osist-pren-50126-1-2012)

3.38**hazard rate**

the rate of occurrence of a hazard

Note 1 to entry: For detailed mathematical understanding of "rate" refer to the definition of "failure rate".

3.39**implementation**

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

3.40**implementer**

the entity that carries out implementation

3.41**independence (functional)**

freedom from any mechanism which can affect the correct operation of more than one function as a result of either systematic or random failure

3.42**independence (physical)**

freedom from any mechanism which can affect the correct operation of more than one system/subsystem/ equipment as a result of random failures

3.43**individual risk**

a risk, resulting from e.g. a product, process or system, to which an individual person is exposed

Note 1 to entry: Individual risk is not to be confused with single victim accidents.

Note 2 to entry: Collective risk is the sum of the individual risks to those individuals in the population or group. However, the collective risk divided by the number of individuals will only provide the average individual risk.

3.44**infrastructure manager**