



DPC: 25/30509666 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 24 January 2025

Origin: European

Latest date for receipt of comments: 19 March 2025

Project No. 2025/00372

Responsible committee: GEL/9/1 Railway Electrotechnical Applications - Signalling and communications

Interested committees:

Title: Draft BS EN 50159 BS Railway Applications - Communication, signalling and processing systems - Safety-related communication in transmission systems.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 19 March 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: William Westcott (BSI)

Direct tel: 020 3142 5692

E-mail: william.westcott@rssb.co.uk

Full document details: 25/30509666 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

January 2025

ICS 35.240.60; 45.020

Will supersede EN 50159:2010; EN 50159:2010/A1:2020

English Version

Railway Applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2025-04-11.

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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye 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: Rue de la Science 23, B-1040 Brussels

Contents

Page

13	European foreword	3
14	Introduction	4
15	1 Scope	5
16	2 Normative references	5
17	3 Terms, definitions and abbreviations	5
18	3.1 Terms and definitions	5
19	3.2 Abbreviations	15
20	4 Reference architecture	16
21	5 Hazards arising from the transmission system	17
22	6 Classification of transmission systems	19
23	6.1 General	19
24	6.2 General aspects of classification	19
25	6.3 Specific aspects for the classification of transmission systems	19
26	6.4 Relationship between transmission systems and the basic message errors	21
27	7 Requirements for safety defences	21
28	7.1 Preface	21
29	7.2 General requirements	22
30	7.3 Specific defences	23
31	7.4 Applicability of defences	29
32	Annex A (informative) Hazards arising from open transmission systems	30
33	A.1 System view	30
34	A.2 Derivation of the basic message errors	31
35	A.3 Network failure modes	32
36	A.4 A possible approach for hazard identification	33
37	A.5 Conclusions	37
38	Annex B (informative) Categories of transmission systems	39
39	B.1 Categories of transmission systems	39
40	B.2 Relationship between the category of transmission systems and basic message errors	39
41	Annex C (informative) Guideline for defences	41
42	C.1 Applications of time stamps	41
43	C.2 Choice and use of safety codes and cryptographic algorithms	42
44	C.3 Safety code	47
45	C.4 Length of safety code	49
46	C.5 Communication between safety-related and non safety-related applications	52
47	Bibliography	54
48		

49 **European foreword**

50 This document [prEN 50159:2025] has been prepared by CLC/SC 9XA “Communication, signalling and
51 processing systems”.

52 This document is currently submitted to the Enquiry.

53 The following dates are proposed:

- | | | |
|---|-------|--|
| <ul style="list-style-type: none"> • latest date by which the existence of this document has to be announced at national level | (doa) | dav + 6 months |
| <ul style="list-style-type: none"> • latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | dav + 12 months |
| <ul style="list-style-type: none"> • latest date by which the national standards conflicting with this document have to be withdrawn | (dow) | dav + 36 months
(to be confirmed or modified when voting) |

54

55 This document will supersede EN 50159:2010. and all of its amendments and corrigenda (if any).

56 prEN 50159:2025 includes the following significant technical changes with respect to EN 50159:2010:

57 Introduction

58 If a safety-related electronic system involves communication of information, the transmission system then
59 forms an integral part of the safety-related system, and it is understood that the end to end communication is
60 safe in accordance with EN 50129.

61 The transmission system considered in this document, which serves the transfer of information between
62 different locations, has in general no particular preconditions to satisfy. It is from the safety point of view not
63 trusted, or not fully trusted.

64 The document is dedicated to the requirements to be taken into account for the communication of safety-
65 related information over such transmission systems.

66 Although the RAM aspects are not considered in this document, it is recommended to keep in mind that they
67 are a major aspect of the operational safety.

68 The safety requirements depend on the characteristics of the transmission system. In order to reduce the
69 complexity of the approach to demonstrate the safety of the system, transmission systems have been
70 classified into three categories:

- 71 – Category 1: transmission systems are closed,
- 72 – Category 2 and Category 3: transmission systems are open.

73 Application messages using Category 3 transmission systems need protection against unauthorised access.
74 The specific cybersecurity requirements for Category 3 transmission systems are out of the scope of this
75 document. For such systems, cybersecurity standards are applicable.

1 Scope

This document is applicable to safety-related electronic systems using for digital communication purposes a transmission system which was not necessarily designed for safety-related applications. For transmission systems where the risk of unauthorized access is not tolerable, the document defines the interface to the applicable cybersecurity standards.

Both safety-related equipment and non-safety-related equipment can be connected to the transmission system.

This document gives the specific requirements needed to achieve safety-related communication between safety-related equipment connected to the transmission system, while the general system requirements including allocation of safety requirements and content of the safety case are defined in EN 50129.

This document is not applicable to existing systems, which had already been accepted prior to the release of this document. However, so far as reasonably practicable, it is applicable to modifications and extensions to existing systems, subsystems and equipment.

This document does not specify

- the transmission system,
- equipment connected to the transmission system,
- solutions (e.g. for interoperability),
- which kind of data are safety-related and which are not.

A safety-related equipment connected through an open transmission system can be subjected to many different IT security threats, against which an overall program is defined, encompassing management, technical and operational aspects.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 50129:2018,¹ *Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling*

CLC/TS 50701:2023, *Railway applications – Cybersecurity*

IEC 63452,² *Rail applications - Cybersecurity*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org>

¹ As impacted by EN 50129:2018/AC:2019-04.

² Under preparation.

3.1.1

absolute time stamp

time stamp referenced to a global time which is common for a group of entities using a transmission system

[SOURCE: IEV 821-11-01]

3.1.2

access control

protection of system resources against unauthorized access

Note to entry: In this document, this definition applies only to data transmission.

[SOURCE: CLC/TS 50701:2023, modified — Note 1 to entry added]

3.1.3

additional data

data which is not of any use to the ultimate user processes, but is used for control, availability, and safety purposes

[SOURCE: IEV 821-11-03]

3.1.4

attack

attempt to gain access to an information processing system in order to produce damage

Note 1 to entry: The damage can be e.g. destruction, disclosure, alteration, disruption, unauthorized use.

Note 2 to entry: In this document, this definition applies only to data transmission.

[SOURCE: CLC/TS 50701:2023, modified — Note 2 to entry added]

3.1.5

authentic message

message in which information is known to have originated from the stated source

[SOURCE: IEV 821-11-04]

3.1.6

authenticity

state in which information is known to have originated from the stated source

[SOURCE: IEV 821-11-05]

3.1.7

closed transmission system

fixed number or fixed maximum number of participants linked by a transmission system with well-known and fixed properties, and where the risk of unauthorised access is negligible

[SOURCE: IEV 821-11-06]

3.1.8

communication

information transfer according to agreed conventions

[SOURCE: IEV 701-01-04]

3.1.9**confidentiality**

<in cybersecurity>

assurance that information is not disclosed to unauthorized individuals, processes, or devices

[SOURCE: CLC/TS 50701:2023]

3.1.10**corrupted message**

type of message error in which a data corruption occurs

[SOURCE: IEC 821-11-08]

3.1.11**countermeasure**

<in cybersecurity>

action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[SOURCE: CLC/TS 50701:2023]

3.1.12**cryptographic algorithm**

algorithm based on the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms

[SOURCE: IEC 62443-1-1]

3.1.13**cybersecurity**

<in railway application>

set of activities and measures taken with the objective to identify, protect, detect, respond, and recover to unauthorised access or cyberattack which could lead to an accident, an unsafe situation, or railway application performance degradation

Note 1 to entry: It is recognized that the term “cybersecurity” has a broader meaning in other standards and guidance, often including non-malevolent threats, human errors, and protection against natural disasters. Those aspects, except human errors degrading security countermeasures, are not included in this document.

[SOURCE: CLC/TS 50701:2023]

3.1.14**cyclic redundancy check**

<for communication in transmission systems>

cyclic code, used to protect messages from the influence of data corruption

[SOURCE: IEC 821-11-10]

3.1.15**data**

<for communication in transmission systems>

part of a message which represents some information (see also user data, additional data, redundant data)

[SOURCE: IEC 821-11-11]

- 189 **3.1.16**
190 **data corruption**
191 alteration of data
- 192 [SOURCE: IEV 821-11-13]
- 193 **3.1.17**
194 **defence**
195 measure incorporated in the design of a safety-related communication system to counter particular hazards
- 196 [SOURCE: IEV 821-11-14]
- 197 **3.1.18**
198 **delayed message**
199 type of message error in which a message is received at a time later than intended
- 200 [SOURCE: IEV 821-11-15]
- 201 **3.1.19**
202 **deleted message**
203 type of message error in which a message is removed from the message stream
- 204 [SOURCE: IEV 821-11-16]
- 205 **3.1.20**
206 **double time stamp**
207 case when two entities exchange and compare their time stamps. In this case the time stamps in the entities
208 are independent of each other
- 209 [SOURCE: IEV 821-11-17]
- 210 **3.1.21**
211 **encryption**
212 <of data>
213 transformation of data in order to hide their semantic content using cryptography
- 214 Note 1 to entry: The reverse process is called decryption.
- 215 Note 2 to entry: In former version of this document the term “enciphering” was used.
- 216 [SOURCE: IEC 60050-171:2019, 171-08-09, modified — Note 2 to entry added]
- 217 **3.1.22**
218 **error**
219 discrepancy between a computed, observed or measured value or condition and the true, specified or
220 theoretically correct value or condition
- 221 Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.
- 222 Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result
- 223 [SOURCE: EN 50129:2018]
- 224 **3.1.23**
225 **failure**
226 loss of ability to perform as required

227 Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to
 228 categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending
 229 upon the field of application.

230 Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to
 231 the cause of failure.

232 Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

233 [SOURCE: EN 50129:2018]

234 **3.1.24**

235 **fault**

236 abnormal condition that could lead to an error in a system

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

238 [SOURCE: EN 50129:2018]

239 **3.1.25**

240 **feedback message**

241 response from a receiver to the sender, via a return channel

242 [SOURCE: IEV 821-11-21]

243 **3.1.26**

244 **hazard**

245 condition that can lead to an accident

246 [SOURCE: EN 50129:2018]

247 **3.1.27**

248 **hazard analysis**

249 process of identifying hazards and analysing their causes, and the derivation of requirements to limit the
 250 likelihood and consequences of hazards to an acceptable level

251 [SOURCE: EN 50129:2018]

252 **3.1.28**

253 **Hazardous event**

254 event that can cause harm

255 Note 1 to entry: A hazardous event can occur over a short period of time or over an extended period of time.

256 [SOURCE: IEV 903-01-04]

257 **3.1.29**

258 **implicit data**

259 additional data that is not transmitted but is known to the sender and receiver

260 [SOURCE: IEV 821-11-12]

261 **3.1.30**

262 **information**

263 knowledge concerning objects, such as facts, events, things, processes, or ideas (including concepts) that,
 264 within a certain context, has a particular meaning

265 Note 1 to entry: Information can be represented for example by signs, symbols, pictures or sounds.

266 [SOURCE: IEV 171-01-01]

267 **3.1.31**

268 **inserted message**

269 type of message error in which an additional message is implanted in the message stream

270 [SOURCE: IEV 821-11-25]

271 **3.1.32**

272 **integrity**

273 <of information>

274 state in which information is complete and not altered

275 [SOURCE: IEV 821-11-26]

276 **3.1.33**

277 **manipulation detection code**

278 function of the whole message without secret key

279 Note to entry: In contrast to a MAC there is no secret key involved. By the whole message is meant also any implicit
280 data of the message which is not sent to the transmission system. The MDC is often based on a hash function.

281 [SOURCE: IEV 821-11-27]

282 **3.1.34**

283 **masqueraded message**

284 type of inserted message in which a non-authentic message is intentionally designed to appear to be
285 authentic

286 [SOURCE: IEV 821-11-28]

287 **3.1.35**

288 **message**

289 <in transmission systems>

290 information which is transmitted in one or several packets from a sender to one or more receivers

291 [SOURCE: IEV 821-11-29]

292 **3.1.36**

293 **message authentication code**

294 cryptographic function of the whole message and a secret or public key

295 Note to entry: By the whole message is meant also any implicit data of the message which is not sent to the
296 transmission system.

297 [SOURCE: IEV 821-11-30]

298 **3.1.37**

299 **message encryption**

300 transformation of bits by using a cryptographic technique within a message, in accordance with an algorithm
301 controlled by keys, to render casual reading of data more difficult

302 Note 1 to entry: Message encryption does not provide protection against data corruption.

303 Note 2 to entry: The original definition was for “message enciphering”. However, in this document, encryption is more
304 common.

305 [SOURCE: IEV 821-11-31, modified — Note 2 to entry added]

- 306 **3.1.38**
 307 **message errors**
 308 set of all possible message failure modes which can lead to potentially dangerous situations, or to reduction in
 309 system availability
- 310 Note 1 to entry: There can be a number of causes of each type of error
- 311 [SOURCE: IEV 821-11-32]
- 312 **3.1.39**
 313 **message integrity**
 314 message in which information is complete and not altered
- 315 [SOURCE: IEV 821-11-33]
- 316 **3.1.40**
 317 **message stream**
 318 ordered set of messages
- 319 [SOURCE: IEV 821-11-34]
- 320 **3.1.41**
 321 **negligible risk**
 322 risk which is so low that it is not reasonable to implement additional measures
- 323 Note 1 to entry: For negligible risks, no further requirements need to be specified. Negligible risks are considered as
 324 insignificant and adequately controlled.
- 325 **3.1.42**
 326 **open transmission system**
 327 transmission system with an unknown number of participants, having unknown, variable and non-trusted
 328 properties, used for unknown telecommunication services and having the potential for unauthorised access
- 329 [SOURCE: IEV 821-11-36]
- 330 **3.1.43**
 331 **random failure**
 332 failure that occurs randomly in time
- 333 [SOURCE: IEV 821-11-38]
- 334 **3.1.44**
 335 **redundancy check**
 336 type of check that a predefined relationship exists between redundant data and user data within a message, to
 337 prove message integrity
- 338 [SOURCE: IEV 821-11-39]
- 339 **3.1.45**
 340 **redundant data**
 341 additional data, derived, by a safety-related transmission function, from the user data
- 342 [SOURCE: IEV 821-11-40]

3.1.46

relative time stamp

time stamp referenced to the local clock of an entity. In general there is no relationship to clocks of other entities

[SOURCE: IEC 821-11-41]

3.1.47

repeated message

type of message error in which a single message is received more than once

[SOURCE: IEC 821-11-42]

3.1.48

re-sequenced message

type of message error in which the order of messages in the message stream is changed

[SOURCE: IEC 821-11-43]

3.1.49

safe fall back state

safe state of a safety-related equipment or system as a deviation from the fault-free state and as a result of a safety reaction leading to a reduced functionality of safety-related functions, possibly also of non safety-related functions

[SOURCE: IEC 821-11-44]

3.1.50

safety

freedom from unacceptable levels of risk

[SOURCE: EN 50129:2018]

3.1.51

safety case

documented demonstration that the product complies with the specified safety requirements

[SOURCE: EN 50129:2018]

3.1.52

safety code

redundant data included in a safety-related message to permit data corruptions to be detected by the safety-related transmission function

Note to entry: Also, codes based on cryptographic algorithms may be used as safety codes such as hash block codes or MAC with fixed keys. For such “keyless” or “fixed key” cryptographic safety codes the same requirements apply.

[SOURCE: IEC 821-11-45] adapted

3.1.53

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 50129:2018]

382 **3.1.54**
 383 **safety reaction**
 384 safety-related protection taken by the safety process in response to an event (such as a failure of the
 385 transmission system), which may lead to a safe fall back state of the equipment

386 [SOURCE: IEC 821-11-47]

387 **3.1.55**
 388 **safety-related**
 389 carries responsibility for safety

390 Note 1 to entry: A function, component, product, system, or procedure is called safety-related if at least one of its
 391 properties is used in the safety argument for the system in which it is applied. These properties can be of functional or
 392 non-functional nature.

393 [SOURCE: EN 50129:2018]

394 **3.1.56**
 395 **safety-related transmission function**
 396 function incorporated in the safety-related equipment to ensure authenticity, integrity, timeliness and sequence
 397 of data

398 **3.1.57**
 399 **sequence number**
 400 additional data field containing a number that changes in a predefined way from message to message

401 [SOURCE: IEC 821-11-48]

402 **3.1.58**
 403 **source and destination identifier**
 404 identifier which is assigned to each entity. This identifier can be a name, number or arbitrary bit pattern. This
 405 identifier will be used for the safety-related communication. Usually the identifier is added to the user data

406 [SOURCE: IEC 821-11-49]

407 **3.1.59**
 408 **systematic failure**
 409 failure that occurs repeatedly under some particular combination of inputs, or under some particular
 410 environmental condition

411 [SOURCE: IEC 821-11-50]

412 **3.1.60**
 413 **threat**
 414 <in cybersecurity>
 415 circumstance or event with the potential to adversely affect operations (including mission, functions, image or
 416 reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure,
 417 modification of data and/or denial of service

418 Note to entry: In this document, this definition applies only to data transmission.

419 [SOURCE: CLC/TS 50701:2023, modified — Note 1 to entry added]

420 **3.1.61**
 421 **time stamp**
 422 representation of information concerning time of transmission attached to a message by the sender

423 [SOURCE: IEC 821-11-52]

424 **3.1.62**

425 **timeliness**

426 state in which information is available at the right time according to requirements

427 [SOURCE: IEV 821-11-53]

428 **3.1.63**

429 **tolerable risk**

430 risk which is accepted in a given context based on the current values of society

431 Note to entry: The terms “acceptable risk” and “tolerable risk” are considered to be synonymous.

432 [SOURCE: IEV 903-01-12]

433 **3.1.64**

434 **transmission code**

435 redundant representation of information, added to the safety and non safety message of the transmission
436 system in order to ensure the integrity of the message during transmission

437 [SOURCE: IEV 821-11-54]

438 **3.1.65**

439 **transmission system**

440 <in communication, signalling and processing systems>

441 service used by the application to communicate message streams between a number of participants, who
442 may be sources or sinks of information

443 [SOURCE: IEV 821-11-55]

444 **3.1.66**

445 **trusted**

446 which has properties used as evidence to support the safety demonstration

447 **3.1.67**

448 **unauthorised access**

449 situation in which user information or information within the transmission system is accessed and/or changed
450 by unauthorised persons

451 [SOURCE: IEV 821-11-56]

452 **3.1.68**

453 **user data**

454 data which represents the states or events of a user process, without any additional data

455 Note 1 to entry: In case of communication between safety-related equipment, the user data contains safety-related data.

456 [SOURCE: IEV 821-11-57]

457 **3.1.69**

458 **valid message**

459 message whose form meets in all respects the specified user requirements

460 [SOURCE: IEV 821-11-58]

461 **3.1.70**
 462 **validity**
 463 state of meeting in all respects the specified user requirements

464 [SOURCE: IEC 821-11-59]

465 **3.2 Abbreviations**

466 For the purpose of this document, the following abbreviations apply.

BCH	Bose, Ray-Chaudhuri, Hocquenghem Code
B.M.E.	Basic Message Errors
BSC	Binary Symmetric Channel
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
EC	European Community
EMI	Electromagnetic Interference
FEC	Forward Error Correction
GPRS	General Packet Radio Service
GSM-R	Global System for Mobile communication – Railways
H.E.	Hazardous Events
HW	Hardware
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentication Code
MDC	Manipulation Detection code
MD4, MD5	Message Digest algorithms
M.H.	Main Hazard
MTBF	Mean Time Between Failures
MVB	Multi-purpose Vehicle Bus
PROFIBUS	Process Field Bus
QSC	q-nary symmetric channel
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
SR	Security Requirement
SRS	Safety Requirements Specifications
SW	Software
TS	Technical Specification
TX	Transmission
UTC	Universal Coordinated Time
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity