SPONSORED BY THE

Federal Ministry
of Education
and Research

INDUSTRIAL RADIO.DE

Aspects of Dependability Assessment in ZDKI

Technical Group 1

"Applications, Requirements and Validation" of the Accompanying Research – Reliable wireless communication in industry (BZKI) in the BMBF Funding Programme "ICT 2020 – Reliable Wireless Communication in Industry" (ZDKI)

www.industrialradio.de

Editor: Sarah Willmann
ifak e.V. Magdeburg
Version: 1.0 (02.06.2017)

Autoren
André Gnad, ifak e.V. Magdeburg
Elke Hintze, ifak e.V. Magdeburg
Marko Krätzig, ifak e.V. Magdeburg
Lutz Rauchhaupt, ifak e.V. Magdeburg

The project on which this report is based has been funded by the Federal Ministry for Education and Research (BMBF) under code number 16KIS0303. The issues concerned were discussed with research partners during the work of Technical Group 1, “Applications, Requirements and Validation” in the BMBF funding programme “ICT 2020 – Reliable Wireless Communication in Industry”.

The authors thank all the research partners who have contributed with their comments to the completeness and comprehensibility of this version.

Contents

List of illustrations

page

List of tables

page

1 Purpose of the document

In the course of the work on the joint projects within the BMBF funding programme “ICT 2020 – Reliable Wireless Communication in Industry, and during discussions in the Technical Groups engaged in coordinating research (BZKI), it has become apparent that the term “reliability” or “dependability” is not being interpreted and applied in a uniform manner. As, however, the assessment of dependability plays a central role in wireless communication into which research is to be conducted in this funding programme, the aspects of dependable wireless communication are examined in this document and made available to the joint projects for consistent use.

This document reveals the variety of existing standards, directives, definitions and variables used in assessing reliability and dependability. That variety is given structure here, and evaluated from the perspective of the application with a view to communication. In the final analysis the aim of finding measurable quantities with which the dependability of wireless communication can be quantitatively assessed is pursued.

2 Definitions, abbreviations and symbols

2.1 Definitions

Data throughput
Number of user data bytes or user data bits per unit of time which are passed to the application by the communication interface in a source.
[Source: [1], modified]

…rate
Factor usually expressed as a percentage or any decimal fraction such as thousandth or millionth
[Source: IEV 112-03-19[2]]

Characteristic parameter
Mathematical parameter for quantitative description of characteristics and states

User data length
Number of indivisible information units which are exchanged at the reference interface
[Source: [3], modified]

Rate/Ratio
Share or proportion which is determined in an individual case or results from ratio calculations.
[Source: [4], modified]

…rate
Quotient of a quantity by a duration
[Source: IEV 112-03-18 [2], modified]

Resilience
Ability of an asset to react independently to disturbances, i.e. automatically to perform the required function again after a disturbance and improve its robustness against the disturbance

Transfer interval
Time difference between two successive transmissions of user data from the automation function via the reference interface to the wireless transmission function
[Source: [3]]

Statistical measure

Statistical parameter of a characteristic parameter, e.g. mean value

Probabilistic measure

Statistical parameter of a characteristic parameter for dependability, e.g. expectation value

Dependability parameter

Characteristic parameter for quantification of dependability

2.2 Abbreviations and symbols

A	Availability
Ad	Address
$a_i(to)$	Availability in observation time
BER	Bit error ratio
c	Correctness
Co	Data content
CRC	Cyclic Redundancy Check
HCL	Higher Communication Layer
IEV	International Electrotechnical Vocabulary
LCL	Lower Communication Layer
$M(O)TBF$	Mean operating time between failures
MDT	Mean down time
MER	Message error rate
Me_{Rxi}	Message received
MLR	Message loss ratio
$MTTF$	Mean operating time to failure
MUT	Mean up time
N_{AFP}	Number of alien packets received
N_{AN}	Number of alien messages received
N_D	Number of communication errors in observation time
N_{Fx}	Number of incorrectly received messages
N_{LM}	Number of lost messages
N_{LP}	Number of lost packets
N_{RCP}	Number of correctly received packets
N_{RFP}	Number of incorrectly received packets
N_{RM}	Number of received messages
N_{Rx}	Number of correctly received messages
N_{TP}	Number of transmitted packets
N_{Tx}	Number of transmitted messages
OSI	Open System Interconnection
OT	Operating time
p	Bit error probability
p_E	Packet error probability
PER	Packet error ratio
PES	Programmable Electronic System
PFD	Probability of dangerous Failure on Demand
PFH	Average frequency of dangerous failure [h-1] per hour
PL	Physical Layer
PLR	Paket loss ratio
$plr_i(to)$	Packet loss ratio in observation time

P_{Ri}	Packets received
R	Residual error probability
$R(t)$	Survival function
RMI	Ratio of message interference
RPI	Ratio of packet interference
SCR	Source
SIL	Safety Integrity Level
SN	Sequence number
TGT	Target
TBF	Operating time between failures
to	Observation time
t_{op}	Operating Time
t_R	Response time
t_T	Transmission time
$TTFF$	Operating time to first failure
t_{TI}	Transfer interval
T_{Tmax}	Maximum limit of transmission time
t_U	Time of error-free data transmission
λ	Failure rate
Λ	Residual error rate
$\overline{\lambda}$	Mean failure rate

3 The concepts of dependability and reliability

3.1 Procedure

In order to identify the essence of the term “dependability”, research was conducted in various sources. General definitions, technical definitions and definitions related to communication are cited. It becomes apparent that different definitions have been established for different professional disciplines, and that these may also differ from country to country. A brief selection of the usual definitions follows.

3.2 General definitions

“Dependability is a characteristic of beings, objects and processes which indicates the extent to which the expected quality or action is provided. Dependability must be repeated verified anew, as it may change in the course of time.” [4]

“You only value your own dependability when you have to rely on others.” [Italian proverb]

“He that is faithful in that which is least is faithful also in much.” [Luke 16.10]

“Dependability can also mean that someone regularly fails.” [Amintore Fanfani]

3.3 Technical definitions

Dependability
“ability to perform as and when required

Note 1 to entry: Dependability includes availability, reliability, recoverability, maintainability, and maintenance support performance, and, in some cases, other characteristics such as durability, safety and security.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.“
[Source: IEV 192-01-22 [2]]

Dependability
"is a collective term for reliability, availability, safety and maintainability."
[Source: [6]]

Dependability
"is the quality of an item with regard to its suitability to fulfil the reliability requirements during or after specified periods of time under specified application conditions."
[Source: [7]]

Dependability
"is the ability of a technical system to satisfy requirements determined by its intended purpose within specified limits and for a stipulated duration."
[Source: [8]]

Dependability
"The dependability of a technical product is a property – behavioural characteristic – which indicates how reliably a function assigned to the product is performed within an interval of time. It is subject to a stochastic process and can be defined qualitatively or quantitatively (in terms of reliability as a measure of the probability of survival) – but is not directly measurable. A distinction is to be made between this and the deterministic properties (characteristics) of a product, which are directly measurable (such as weight, dimensions, strength, colour, electrical and thermal conductivity)."
[Source: [9]]

Reliability
"The ability of an item to perform a required function under given conditions for a given time interval."
[Source: [10]]

Reliability
"The probability that an automated system can perform a required function under given conditions for a given time interval ($t1$, $t2$)"
[Source: [11]]

Reliability of an item
"The ability of an item to perform a required function under stated conditions for a specified period of time."
[Source: IEV 603-05-01 [2]]

Reliability
Is the ability of an item to fulfil a required function under given conditions for a given period of time. Reliability can on the one hand be defined qualitatively, or on the other hand quantitatively as the probability of survival."
[Source: [6]]

3.4 Definitions in telecommunication

With regard to telecommunication, reliability means that messages are transmitted with an intended Quality of Service (QoS). [12].

The following are extracts from ITU-R, ITU-T and ETSI Recommendations.

Reliability
- "probability that a required performance is achieved"
- "is a figure of merit of performance"

[Source: [13]]

Reliability
"The probability that a product or system will perform as required for a specified period of time."
[Source: [14]]

Reliability
"ability of an item to perform a required function under stated conditions for a given time period

Note 1: It is generally assumed that the item is in a state to perform this required function at the beginning of the time interval."
[Source: [15]]

Reliability (%)
"The amount of sent network layer packets successfully delivered to a given node within the time constraint required by the targeted service, divided by the total number of sent network layer packets."
[Source: [16]]

3.5 Conclusion

The definitions collected here represent a selection which, however, already allows the following conclusions to be drawn:

1. The term “dependability” denotes a parameter which can be measured or calculated. Furthermore, it is a generic term. It groups various performance characteristics together which can be quantified with the aid of various parameters depending on the context.

2. Dependability parameters describe not only the proportion of fault-free functioning, but also the readiness to function and the ability to preserve and restore the function.

3. Dependability parameters are random variables which describe stochastic processes. Consequently, the tools of mathematical statistics are to be used to characterize them.

The second conclusion makes it clear that dependability parameters are not only useful for the static assessment of a system, but also for evaluation of operating conditions and the opportunities for preserving or restoring perfect function. That makes the dependability parameters a decisive factor in the design of resilient systems.

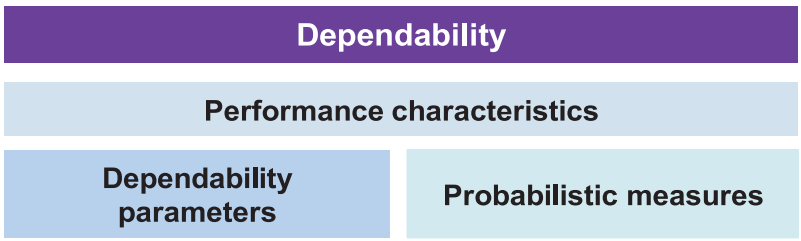


Figure 1: Dependability, performance characteristics and probabilistic measures

The classification by performance characteristics, dependability parameters and probabilistic measures of dependability in figure 1 is based on [18], p. 91.

In the following section, as the basis of a common understanding, the performance characteristics, characteristic parameters and probabilistic measures for assessment of dependability are described.

4 Performance characteristics, characteristic parameters and probabilistic measures for assessment of dependability

4.1 General

Relevant performance characteristics, characteristic parameters and probabilistic measures for assessment of dependability are taken from the literature and presented here. The terms used are not thoroughly consistent, as they are quoted from various sources. The quotations have consciously not been adjusted for consistency here. Only when the terms are applied to communication items in Sections 6 and 7 is attention paid to uniformity.

4.2 Performance characteristics

4.2.1 Availability

Availiability
“ability to be in a state to perform as required

Note 1 to entry: Availability depends upon the combined characteristics of the reliability, recoverability, and maintainability of the item, and the maintenance support performance.

Note 2 to entry: Availability may be quantified using measures defined in Section 192-08, Availability related measures”
[Source: IEV 192-01-23 [2]

Availiability
“Availability of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided.”
[Source: Definition 3.1.1.5.4 [19]]

4.2.2 Reliability

Reliability
“ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run. Etc., and the units should always be clearly stated.

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 may be quantified using measures defined in Section 192-05, Reliability related concepts: measures.”
[Source: IEV 192-01--24 [2]]
Similar entries: IEV 312-07-06, IEV 395-07-131

4.2.3 Recoverability

Recoverability
“ability to recover from a failure, without corrective maintenance

Note 1 to entry: The ability to recover may or may not require external actions. For recovery where no external actions are required, see self-recoverability (192-01-26).

Note 2 to entry: Recoverability may be quantified using measures such as the probability of recovery within a specified time interval.”
[Source: IEV 192-01-25 25 [2]]

4.2.4 Self-recoverability

Self-recoverability
“ability to recover from a failure, without external action
Note 1 to entry: Self-recoverability is a special case of recoverability (192-01-25).”
[Source: IEV 192-01-26 [2]]

4.2.5 Maintainability

Maintainability
"ability to be retained in, or restored to a state to perform as required , under given conditions of use and maintenance

Note 1 to entry: Given conditions would include aspects that affect maintainability, such as: location for maintenance, accessibility, maintenance procedures and maintenance resources.

Note 2 to entry: Maintainability may be quantified using measures defined in Section 192-07, Maintainability and maintenance support: measures."
[Source: IEV 192-01-27 [2]]

4.2.6 Maintenance support performance

Maintenance support performance
"effectiveness of an organization in respect of maintenance support

Note 1 to entry: Maintenance support performance may be quantified using measures defined in Section 192-07, Maintainability and maintenance support: measures"
[Source: IEV 192-01-29 [2]]

4.2.7 Durability

Durability
"ability to perform as required, under given conditions of use and maintenance, until the end of useful life"
[Source: IEV 192-01-21 [2]]

4.2.8 Security/Safety

Security/Safety
"freedom from unacceptable risk to the outside from the functional and physical units considered

Note 1 to entry: The definition of "safety" in combination with other words may gradually (as in "product safety", "machinery safety") or completely (as in "workers safety", "safety belt" or "functional safety") change. Regard IEC Guide 51 cl. 4 to the use of the word safety. [ISO/IEC Guide 2, Standardization and related activities – General vocabulary]

Note 2 to entry: In standardization the safety of products, processes and services is generally considered with a view to achieving the optimum balance of a number of factors, including non-technical factors such as human behaviour, that will eliminate avoidable risks of harm to persons and goods to an acceptable degree. [ISO/IEC Guide 2]

Note 3 to entry: In many other languages than English there is only one word for safety and security."
[Source: IEV 351-57-05 [2]]

Information security
"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."
[Source: [40]]

Functional safety
"part of the overall safety that depends on functional and physical units operating correctly in response to their inputs"
[Source: IEV 351-57-06 [2]]

4.2.9 Quality of service

Quality of service

"The collective effect of service performances which determine the degree of satisfaction of a user of the service

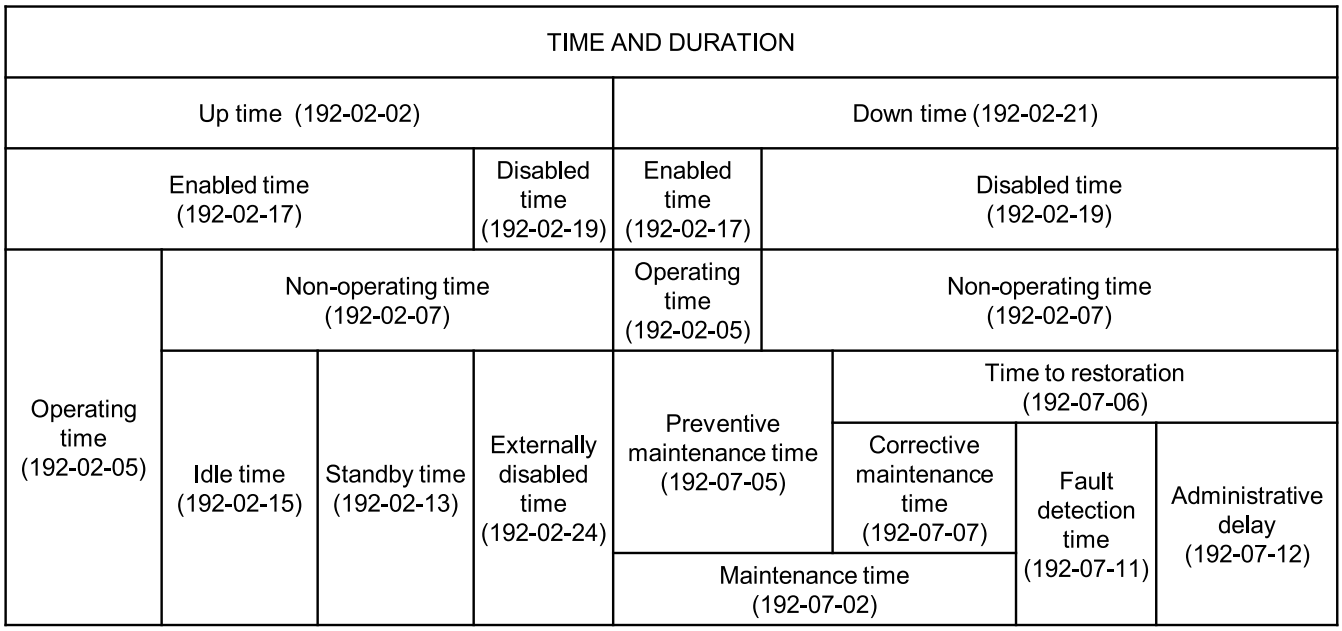
Note: These characteristic performances may, for example, relate to: transmission quality, dial-tone delay, failures, fault frequency and duration."

[Source: IEV 715-07-14 [2]]

4.3 General dependability parameters

4.3.1 Overview

Figure 2 shows the relationships between fundamental terms of time and duration used for the characterization of the operation and maintenance of items. A number of these terms are defined on the following pages, as they can be used as dependability parameters.



Note 1: All time parameters mentioned in this picture are time intervals or successive time intervals.

Figure 2: Time-related terms for characterization of operation and maintenance [2]

4.3.2 Up time

Up time
"time interval for which the item is in an up state"
[Source: IEV 192-02-02 [2]]

4.3.3 Operating time

Operating time
"time interval for which an item is in an operating state

Note 1 to entry: The duration of operating time may be expressed in units appropriate to the item concerned, e.g. calendar time, operating cycles, distance run, etc., and the units should always be clearly stated."
[Source: IEV 192-02-05 [2]]

4.3.4 Down time

Down time
"time interval for which the item is in a down state

Note: Down time excludes disabled time due to lack of external resources, but includes maintenance time."
[Source: IEV 192-02-21 [2]]

4.3.5 Operating time to failure

Operating time to failure
"operating time accumulated from the first use, or from restoration, until failure

Note 1 to entry: See also operating time (192-02-05)."
[Source: IEV 192-05-01 [2]]

4.3.6 Time between failures

Time between failures
"duration between consecutive failures

Note 1 to entry: The time between failures includes the up time and the down time."
[Source: IEV 192-05-03 [2]]

4.3.7 Operating time between failures

Operating time between failures
"operating time accumulated between consecutive failures

Note 1 to entry: Operating time between failures is a special case of operating time to failure, applicable only to repairable items."
[Source: IEV 192-05-04 [2]]

4.3.8 Operating time to first failure

Operating time to first failure
"operating time accumulated from the first use until failure

Note 1 to entry: Operating time to first failure is a special case of operating time to failure (192-05-01).

Note 2 to entry: In the case of non-repairable items, the operating time to first failure is the operating time to failure (192-05-01)."
[Source: IEV 192-05-02 [2]]

4.3.9 Restart time

Restart time
"The time taken for a telecontrol system to become fully operational following a power supply failure."
[Source: IEV 371-08-22 [2]]

4.4 Differences and relationships between the dependability parameters

The following figures are intended to provide for better distinctions between the characteristic parameters and their relationships. Figure 3 shows the up time, operating time and down time.

The up state contains an active state (operating state) and an inactive state (idle state). Therefore, operating states can be interrupted by idle states during the up state. Should a fault occur, the up state changes to the down state. The down state continues till maintenance or restoration takes place.

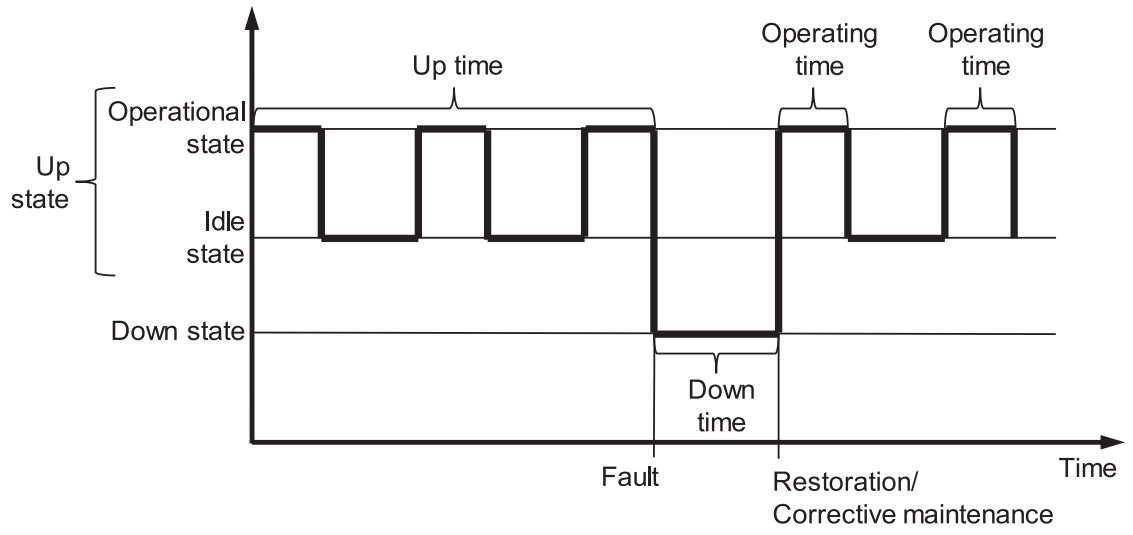


Figure 3: Relationship between up time, operating time, idle time and down time, based on [18]

Figure 4 shows the time between failures and the operating time (*OT*) The operating time to first failure (*TTFF*) and the operating time between failures (*TBF*) result from the total of the individual operating times in the relevant periods, i.e. the operating times within a time between failures.

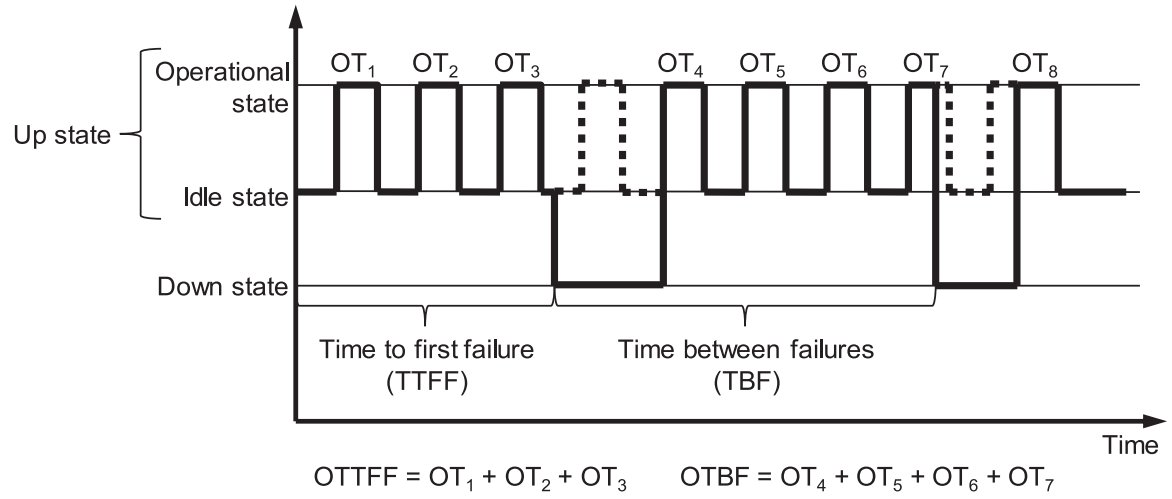


Figure 4: Relationship between time between failures, operating time, operating time to first failure and operating time between failures

It may not be possible for measuring instruments to detect a failure which occurs in the idle state immediately. The down state is only detected when expected operation fails to take place. This case is shown in Figure 5.

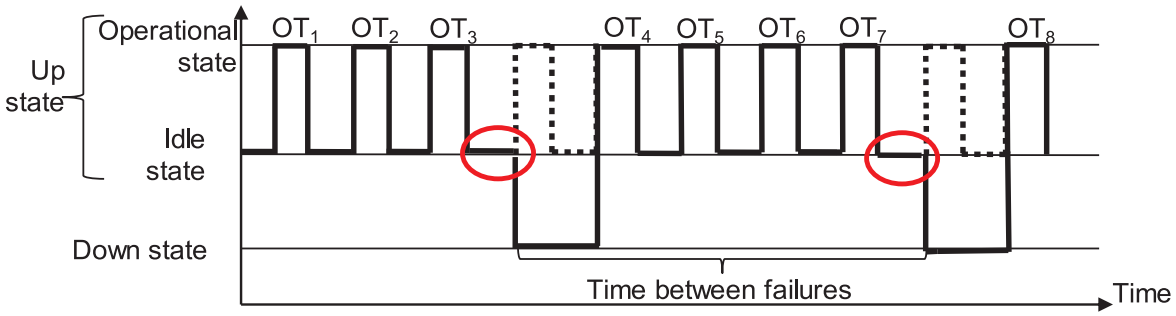


Figure 5: System states and their mapping by measured values of characteristic parameters

The restart time (*RT*) is part of the down time. It is the period which is required to restore the up state after a fault (see Figure 6).

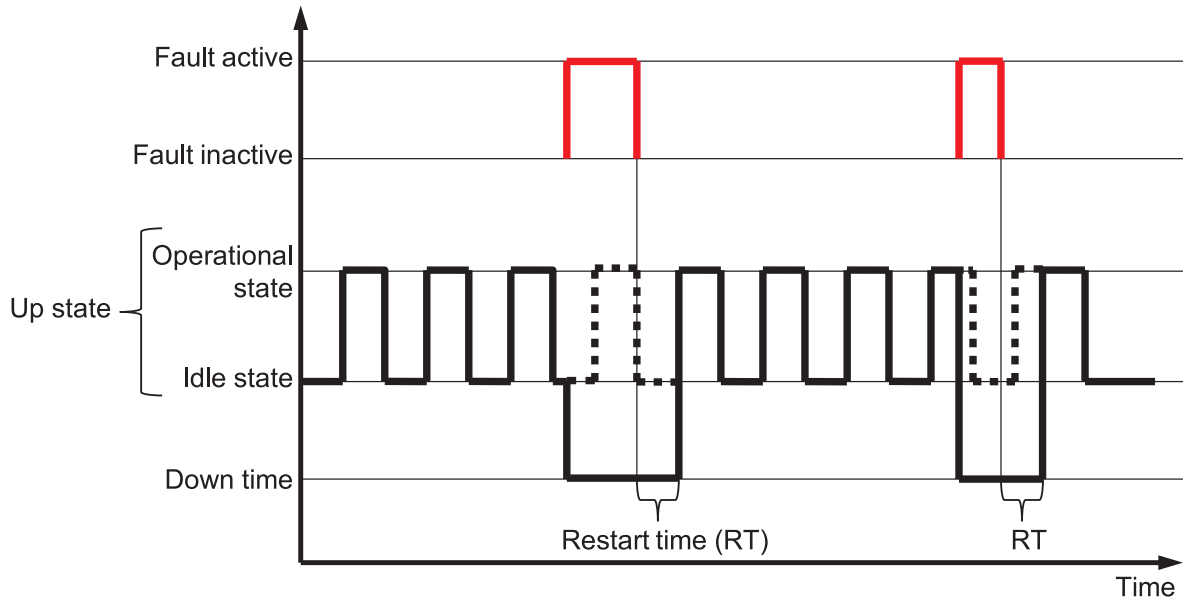


Figure 6: Relationship between faults, down time and restart time (*RT*)

4.5 General probabilistic measures

4.5.1 Availability

Instantaneous availability

"probability that an item is in a state to perform as required at a given instant"

[Source: IEV 192-08-01 [2]]

Inherent availability

"availability provided by the design under ideal conditions of operation and maintenance"

[Source: IEV 192-08-02 [2]]

Operational availability

"availability experienced under actual conditions of operation and maintenance"

[Source: IEV 192-08-03 [2]]

Mean/Average availability

"average value of the instantaneous availability over a given time interval (t_1, t_2)

Note 1 to entry: The mean availability is related to the instantaneous availability $A(t)$ as:

$$\overline{A}(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)dt \qquad (1)"$$

[Source: IEV 192-08-05 [2]]

4.5.2 Reliability

Reliability
"probability of performing as required for the time interval (t_1, t_2) under given conditions

Note 1 to entry: Given conditions include aspects that affect reliability, such as mode of operation; stress levels; environmental conditions; and maintenance, where applicable.

Note 2 to entry: It is usually assumed that the item is in a state to perform as required at the beginning of the time interval.

Note 3 to entry: When t_1 = 0 and t_2 = t, then $R(0,t)$ is denoted simply as $R(t)$ and termed the reliability function, or survival function of the item. See IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms, for more details.

Note 4 to entry: See also reliability, <of an item> (192-01-24)"
[Source: IEV 192-05-05 [2]]

Reliability function (survival function) $R(t)$
Probability of fulfilment of the function by time t, where $R(t) = R(t_1, t_2)$ for t_1 = 0 und t_2= t [17]

4.5.3 Up time distribution function $F_U(t)$

Up time distribution function $F_U(t)$
Function which assigns to each value of t the probability that the duration of up time is less than or equal to t [17]

4.5.4 Complement of the up time distribution function $R_U(t)$

Complement of the up time distribution function $R_U(t)$
Function which assigns to each value of t the probability that the duration of up time is greater than t.

Note 1: $R_U(t) = 1 - F_U(t)$

Note 2: If the durations of the up times are distributed exponentially: $R_U(t) = e^{\frac{-t}{MUT}}$

where MUT is the mean up time. [17]

4.5.5 Failure rate

(Instantaneous) failure rate
"limit, if it exists, of the quotient of the conditional probability that the failure of a non-repairable item occurs within time interval (t, $t + \Delta t$) by Δt, when Δt tends to zero, given that failure has not occurred within time interval (0,t).

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \frac{F(t+\Delta t) - F(t)}{R(t)} = \frac{f(t)}{R(t)} \quad (2)$$

where $F(t)$ and $f(t)$ are, respectively, the distribution function and the probability density at the failure instant, and where $R(t)$ is the reliability function , related to the reliability $R(t_1, t_2)$ by $R(t) = R(0,t)$

Note 1 to entry: See IEC 61703, Mathematical expressions for reliability, availability, maintainability and maintenance support terms, for more detail.

Note 2 to entry: Other terms used for instantaneous failure rate are: “hazard function”; “hazard rate”; and “force of mortality” (abbreviation FOM).”
[Source: IEV 192-05-06 [2]]

Mean/Average failure rate
“average value of the instantaneous failure rate over a given time interval (t_1, t_2)
[Source: IEV 192-05-07 [2]]

$$\bar{\lambda}(t_1, t_2) = \frac{1}{t_1 - t_2} \int_{t_1}^{t_2} \lambda(t) dt \qquad (3)”$$

4.5.6 Mean operating time to failure

Mean operating time to failure (*MTTF*)
“expectation of the operating time to failure

Note 1 to entry: In the case of non-repairable items with an exponential distribution of times to failure (i.e. a constant failure rate) the *MTTF* is numerically equal to the reciprocal of the failure rate. This is also true for repairable items if after restoration they can be considered to be “as-good-as-new”.

Note 2 to entry: See also operating time to failure (192-05-01)”
[Source: IEV 192-05-11 [2]]

4.5.7 Mean operating time between failures

Mean operating time between failures (*MTBF, MOTBF*)
“expectation of the duration of the operating time between failures

Note 1 to entry: Mean operating time between failures should only be applied to repairable items. For non-repairable items, see mean operating time to failure (192-05-11).”
[Source: IEV 192-05-13 [2]]

4.5.8 Mean up time

Mean up time (*MUT*)
“expectation of the up time”
[Source: IEV 192-08-09 [2]]

4.5.9 Mean down time

Mean down time (*MDT*)
“expectation of the down time”
[Source: IEV 192-08-10 [2]]

4.6 Conclusion

The terms defined in this section can be used to firm up Figure 1. Figure 7 shows the assignment of the performance characteristics, dependability characteristics and probabilistic measures, based on [18], p. 91.

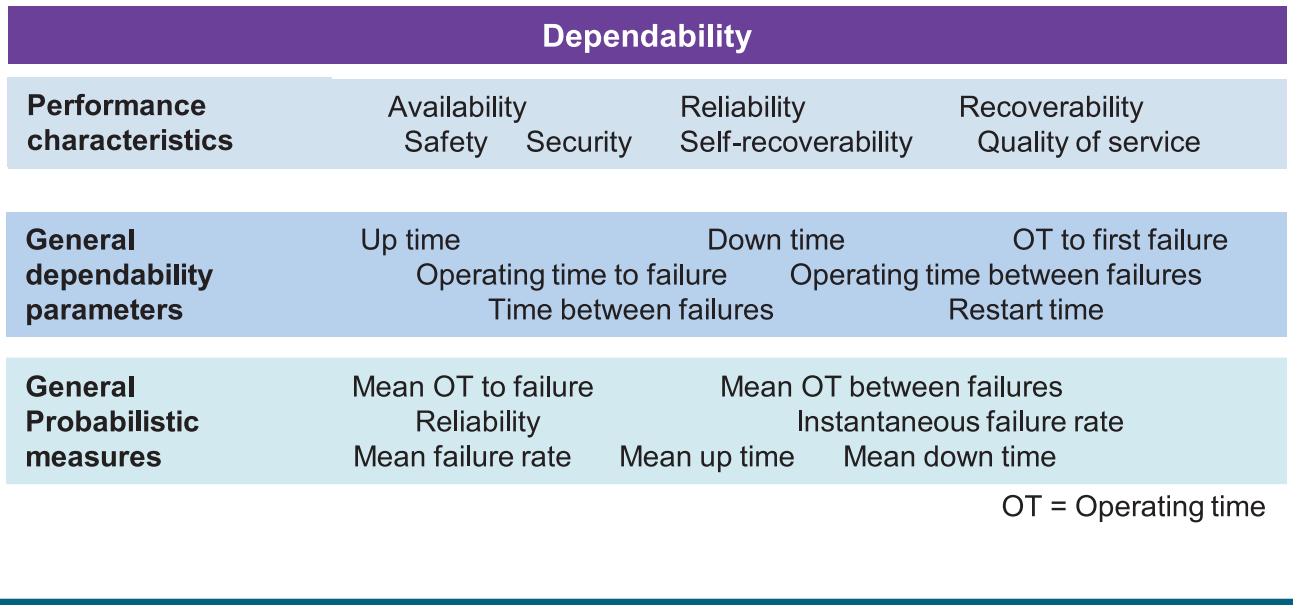


Figure 7: Performance characteristics, characteristic parameters and probabilistic measures of dependability

5 Area of consideration for industrial radio communication

5.1 Area of consideration

In order to apply the concept of dependability to wireless communication in industry, the definition of the area of consideration for industrial radio communication adopted in [20] is to be used (see Figure 8).

The starting point is the necessity of transmitting messages between spatially distributed application functions of an industrial automation application. For that process, messages are exchanged at an interface between the application system and the radio communication system. This interface is termed the reference interface, as required and guaranteed values for characteristic parameters which describe the behavioural properties of the radio communication system refer to that interface. These characteristic parameters include the dependability parameters of industrial radio communication, which are defined in Section 6 for a logical link on the basis of the characteristic parameters listed in Section 4.

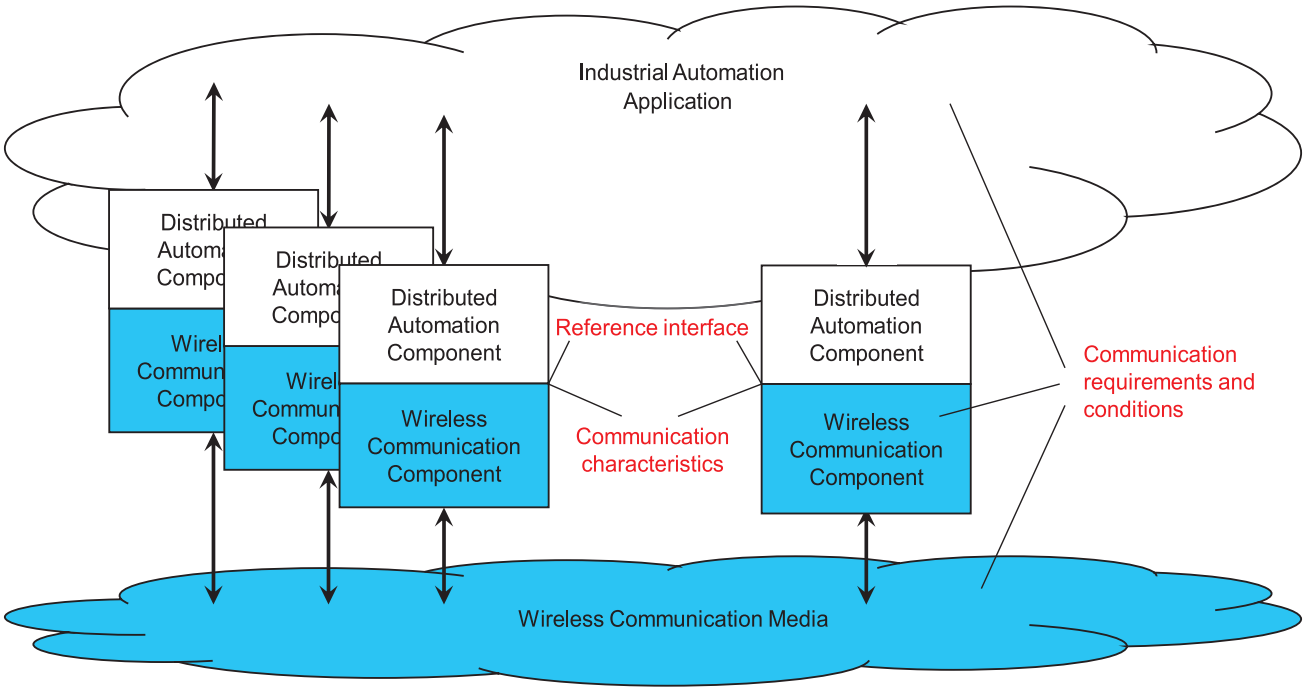


Figure 8: Abstract diagram of the area of consideration for industrial radio communication

The conditions which influence the behaviour of wireless communication are determined by

- the communication requirements of the application (e.g. length of the message),
- the characteristics of the communication system (e.g. output power of a transmitter), and
- the transmission conditions of the media (e.g. signal changes caused by multipath propagation).

The area of consideration shown in Figure 8 represents the general view of an industrial user of radio communication systems.

If a dependability assessment is to be performed, it is necessary in accordance with the definition of the concept of dependability to specify an item, its function and the conditions under which the function is to be performed. Accordingly, these aspects are discussed for relevant units of consideration on the following pages.

General requirements from the application point of view for the time and failure behaviour of a communication system are mostly related to an end-to-end link. It is assumed in this connection that the behaviour of the link is representative of the communication system as a whole and of the entire scope of the application. Depending on the objective or context, this assumption can lead to false conclusions or to misunderstandings. Consequently, the units of consideration which are relevant to dependability assessments are to be discussed on the following pages.

5.2 Logical link

5.2.1 Nature and function

Starting with the general approach mentioned above, the logical link can be regarded as a possible item within the area of consideration (see Figure 9). This is the link between a logical end point in a source device and the logical end point in a target device. Logical end points are elements of the reference interface, which may group several logical end points together. The nature of this view is the reference to the application and the encapsulation of the data transmission.

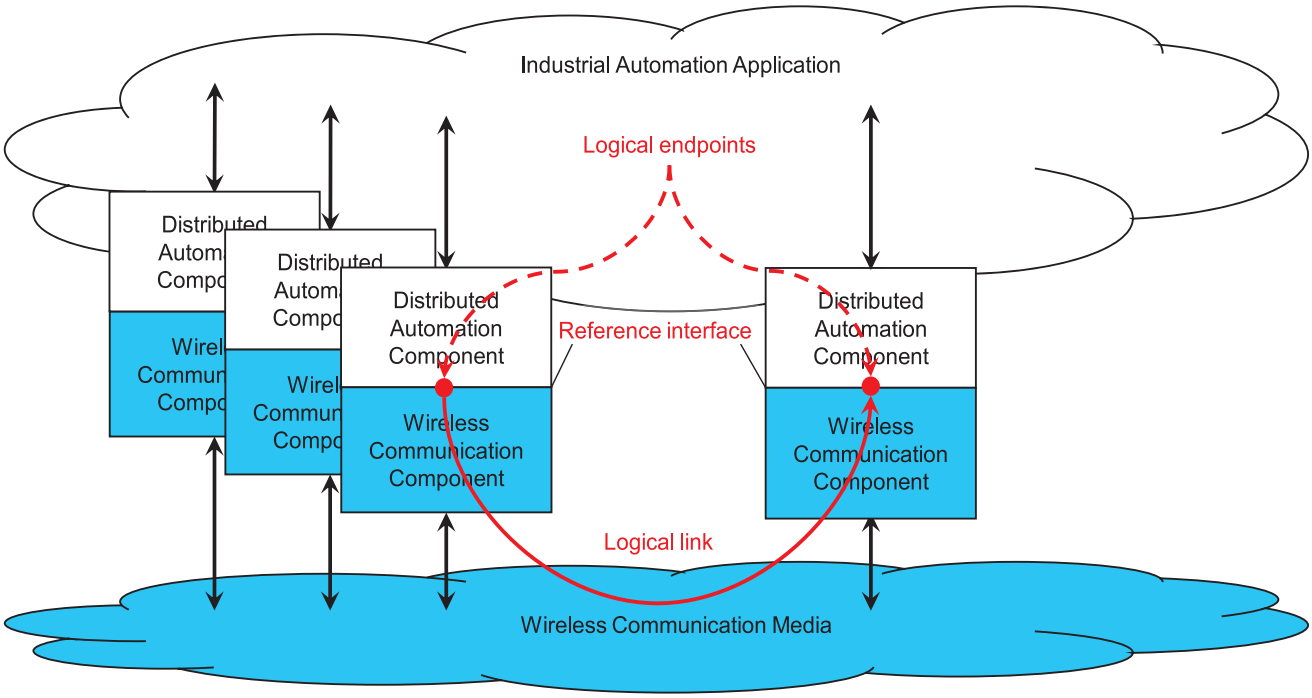


Figure 9: Logical link in the area of consideration

The intended function of the logical link is the transmission of a sequence of messages from a logical source end point to the correct logical target end point. This is achieved by transforming each message into a form which enables error-free transmission. The transmission process includes certain processes, e.g. repetitions, in order to fulfil the intended function. After transmission, the message is converted back into a form which is usable by the application. The message is to be correctly received and available at the target device within a defined time. The sequence of messages at the target is to be the same as the sequence at the source.

The functional units which are necessary to fulfil this function are shown in Figure 10.

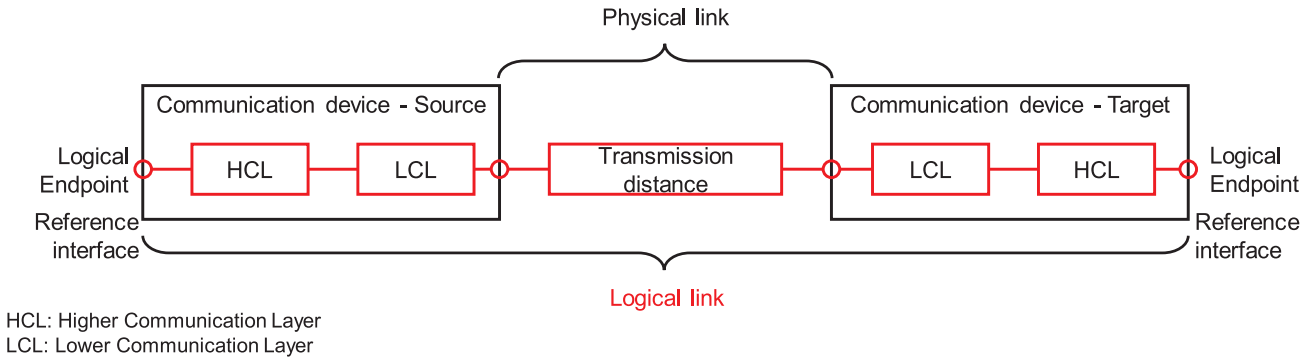


Figure 10: “Logical link” item

The required function can be impaired by various influences, which can lead to communication errors. Such errors are for example described in [20] and [21]. The occurrence of one of these errors influences the values of the relevant dependability parameters of the logical link.

5.2.2 Message transformation

From an implementation point of view, it is hardly possible to identify communication layers and interfaces in devices in a uniform manner, e.g. with reference to the Open System Interconnection (*OSI*) model. However, the implementation of communication functions is mostly split between a higher communication layer (*HCL*) and a lower communication layer (*LCL*), which may contain different parts of the *OSI* reference model from implementation to implementation. The further observations are therefore based on a generic implementation view with *HCL* and *LCL*.

The messages to be transmitted for the intended function of a logical link are defined by strings of characters with a particular semantic content. Such a character string is handed over as user data at the reference interface for transmission. If the number of characters in a message is too great for it to be transmitted as a unit, the message can be divided for transmission into several packets (fragmentation). The packets are then passed from a higher communication layer (*HCL*) to a lower communication layer (*LCL*) (Figure 11). There, a bit steam is created and handed over to the physical layer (*PL*). A signal stream corresponding to the bit stream is transmitted from the physical layer of the source device to the target device. In the target device, the signal stream received is converted by physical layer into a bit stream, which is passed to the lower communication layer. There, packets are formed, handed over by the lower communication layer to the higher communication layer and grouped together there into a message. Suitable mechanisms (acknowledgement), parallel transmission through different communication channels/media, multiple transmissions of identical packets, etc.) can increase the probability of the message reaching the application correctly when a packet is lost. Figure 11 shows the transmission of a message with three packets, including acknowledgement. If no acknowledgement is received within the required period (packet 2), the packet is transmitted again.

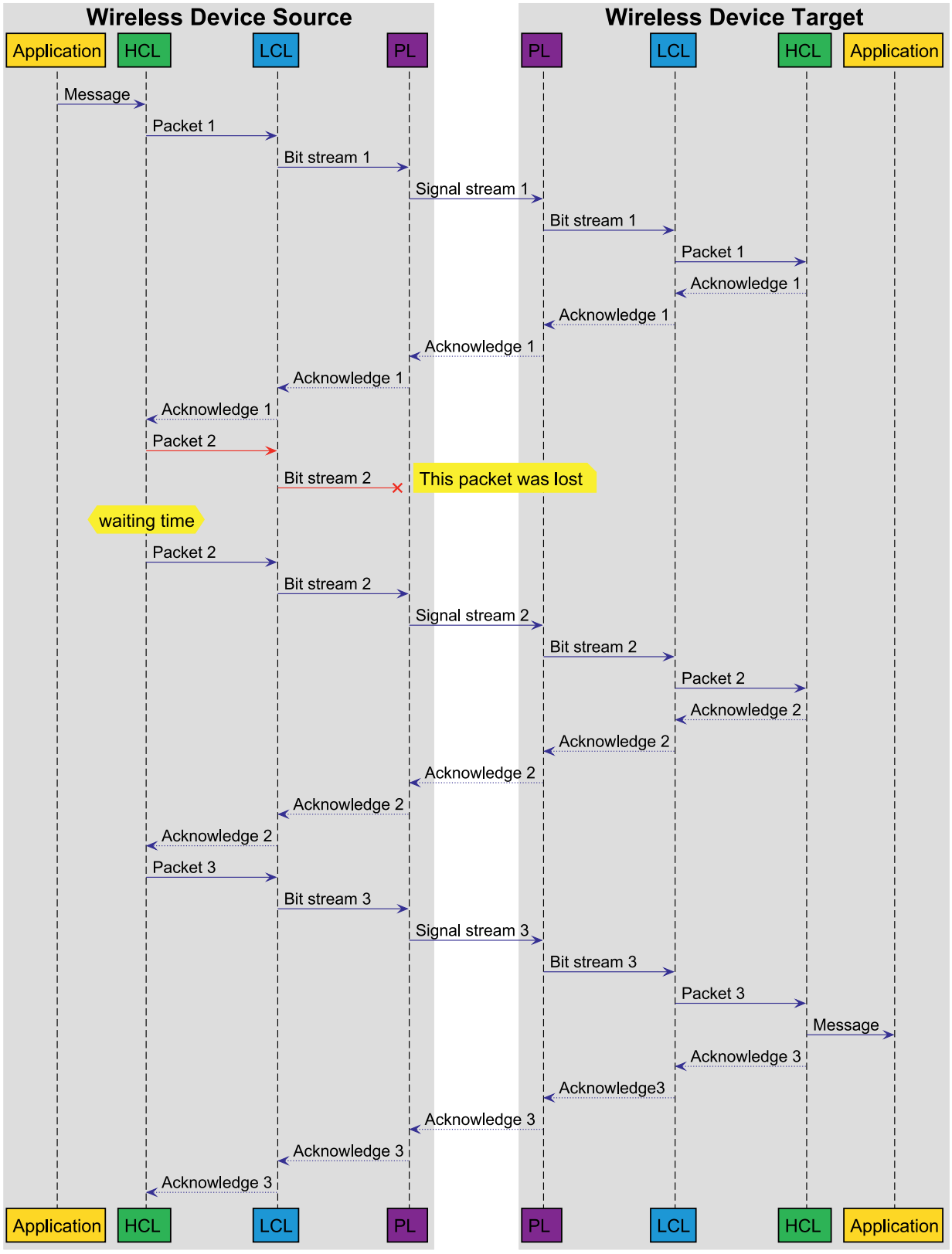


Figure 11: Transmission of a message as packets and bit streams

The loss of a packet is therefore not to be equated in all cases with the loss of a message.

This document focuses on the application-related messages. For better classification, definitions concerning packets can be found in Section 7.

5.2.3 Communication errors

IEC/EN 61784-3-3 [11] describes fundamental communication errors which can be identified for applications with functional safety requirements. The description of these communication errors refers to field buses. These errors may however also occur in other communication systems.

Corruption

Messages may be corrupted due to errors within a bus participant, due to errors on the transmission medium, or due to message interference.

Note 1: Message error during transfer is a normal event for any standard communication system, such events are detected at receivers with high probability by use of a hash function and the message is ignored.

Note 2: Most communication systems include protocols for recovery from message errors, so these messages will not be classed as 'Loss' until recovery or repetition procedures have failed or are not used.

Note 3: If the recovery or repetition procedures take longer than a specified deadline, a message is classed as 'Unacceptable delay'.

Note 4: In the very low probability event that multiple errors result in a new message with correct message structure (for example addressing, length, hash function such as CRC, etc.), the message will be accepted and processed further. Evaluations based on a message sequence number or a time stamp can result in fault classifications such as Unintended repetition, Incorrect sequence, Unacceptable delay, Insertion. [11]

Unintended repetition

Due to an error, fault or interference, old not updated messages are repeated at an incorrect point in time.

Note 1: Repetition by the sender is a normal procedure when an expected acknowledgment/response is not received from a target station, or when a receiver station detects a missing message and asks for it to be resent.

In some cases, the lack of response can be detected and the message repeated with minimal delay and no loss of sequence, in other cases the repetition occurs at a later time and arrives out of sequence with other messages.

Note 2: Some field buses use redundancy to send the same message multiple times or via multiple alternate routes to increase the probability of good reception. [11]

Incorrect sequence

Due to an error, fault or interference, the predefined sequence (for example natural numbers, time references) associated with messages from a particular source is incorrect.

Note 1: Field bus systems can contain elements that store messages (for example FIFOs in switches, bridges, routers) or use protocols that can alter the sequence (for example by allowing messages with high priority to overtake those with lower priority).

Note 2: When multiple sequences are active, such as messages from different source entities or reports relating to different object types, these sequences are monitored separately and errors can be reported for each sequence. [11]

Loss

Due to an error, fault or interference, a message or acknowledgment is not received. [11]

Unacceptable delay

Messages may be delayed beyond their permitted arrival time window, for example due to errors in the transmission medium, congested transmission lines, interference, or due to bus participants sending messages in such a manner that services are delayed or denied (for example FIFOs in switches, bridges, routers).

Note: In underlying field buses using scheduled or cyclic scans, message errors can be recovered in the following several ways:

a) immediate repetition;
b) repetition using spare time at the end of the cycle;
c) treating the message as lost and waiting for the next cycle to receive the next value.

In case a) all the following messages in that cycle are slightly delayed, while in case b) only the resent message gets a delay.

Cases a) and b) are not normally classed as an Unacceptable delay.

Case c) would be classed as an Unacceptable delay unless the cycle repetition interval is short enough to ensure that delays between cycles are not significant and the next cyclic value can be accepted as a replacement for the missed previous value. [11]

Masquerade

Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a non-safety related message may be received by a safety related participant, which then treats it as safety related.

Note: Communication systems used for safety-related applications can use additional checks to detect masquerade, such as authorized source identities and pass-phrases or cryptography. [11]

Insertion

Due to a fault or interference, a message is received that relates to an unexpected or unknown source entity.

Note: These messages are additional to the expected message stream, and because they do not have expected sources, they cannot be classified as Correct, Unintended repetition, or Incorrect sequence. [11]

Addressing

Due to a fault or interference, a safety related message is delivered to the incorrect safety related participant, which then treats reception as correct. [11]

5.3 Communication device

The communication devices essentially determine the function and thus the dependability of the logical link (Figure 12). If communication devices are used as an item in a dependability assessment, the focus is on the methods and algorithms and their implementation. The function of the communication devices is the correct sending and correct receipt of sequences of messages. The methods and algorithms implemented in the communication devices should take the best possible account of the transmission conditions which obtain during message transmission, and fulfil the requirements for message transmission as well as possible. In the context of the ZDKI research tenders, research into corresponding wireless transmission methods for industrial automation constitutes the major focus of the sub-projects.

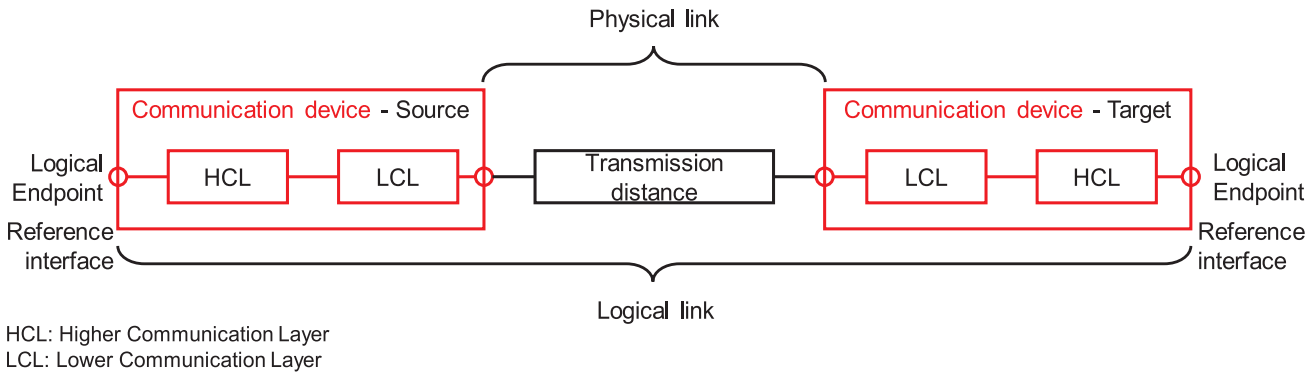


Figure 12: “Communication device” item

Apart from the methods and algorithms themselves, their implementation in hardware and software is also of importance. The errors listed below can have an impact on dependability.

Hardware errors

Hardware errors encompass the failure or disturbance of the function of electrical, electronic and programmable components. They are caused by physical and chemical processes which take place constantly in the environment or in the system. If the function of a component no longer meets the specification, it is as a rule assessed as unusable and therefore as failed.

Depending on the cause, the scope and the speed of occurrence, distinctions are made between:

- Random failure and deterministic failure
- Total failure and partial failure
- Sudden failure and degradation failure, and fatigue failure

Hardware errors may be caused, for example, by

- poor workmanship,
- components of sub-standard quality,
- ageing,
- overloading (e.g. clock frequency, voltage or current),
- high or low temperatures,
- frequent temperature changes,
- impacts, acceleration or vibration,
- electrical, magnetic or electromagnetic fields,
- cosmic radiation, and
- nuclear radiation.

In the context of the ZDKI research tender, there is also a focus on circuitry aspects which are aimed at minimizing malfunctions.

Software errors or program errors

Software errors or program errors encompass the malfunction of computer programs. Distinctions are made between the following kinds of software error:

- Syntax errors
  are infringements of the grammatical rules of the programming language used. A syntax error prevents compilation of the defective program. Syntax errors are not as a rule of interest in run time, unless a programming language which interprets the program sequentially is used.
- Run time errors
  designate all kinds of errors which occur during running of the program, for instance exceeding the value range or incorrect data types for variables on input, when there is no verification or an incorrect version of the operating system is used.
- Logical errors
  occur with an incorrect entry or incorrect algorithm.
- Design errors
  are errors in the basic concept which are caused by the assumption of incorrect requirements or defective software design.
- Errors as a consequence of physical operating conditions
  Electromagnetic fields, radiation, mechanical stresses, temperature fluctuations, etc. can lead to errors even in systems which are working within the specification. One example of this is the change in state of one or more bits in a memory as a result of the influences listed above.

Considerations of software and hardware errors can be found, for example, in IEC 62439 [22], which also deals with concepts of redundancy in industrial Ethernet networks, or in IEC 62673 [23], in which a general methodology for dependability assessment and assurance in communication networks throughout their life cycles is described.

In the context of the ZDKI research tender, procedures for dependable software development are not in the focus.

5.4 Physical link

In wireless transmission, the physical link presents a special challenge. The environment in which it is used has a great influence on the dependability parameters. A distinction is made between passive influences (where the signal transmitted is influenced on the way to the target device) and active influences (where additional signals impair recognition of the useful signal at the target device). The passive influences include the distance (distance-related attenuation of the signal), metallic obstacles (reflection, diffraction and refraction of the signal), dielectric obstacles (attenuation of the signal) and heavy rain or fog (absorption of the signal). Active influences result from the transmission of electromagnetic waves in the vicinity. The passive and active influences are referred to as disturbances. These disturbances have an effect on the physical link and can be the cause of transmission errors.

The dependability assessment of the physical link describes the conditions on which the development of communication methods and algorithms can be based. The function of the physical link is fault-free signal transmission between the physical end point of the source and the physical end point of the target (see Figure 13). With the change of a condition, e.g. the occurrence of an interference signal, interfering objects or a sudden change in the weather, there is an impact on the transmission in the radio transmission medium. The change in conditions may be very rapid, very extensive and almost unpredictable. The transmission errors arising in this way are caused by changes in the signal parameters, with the result that the algorithms and their implementation are unable to reconstruct the information content perfectly at the target device.

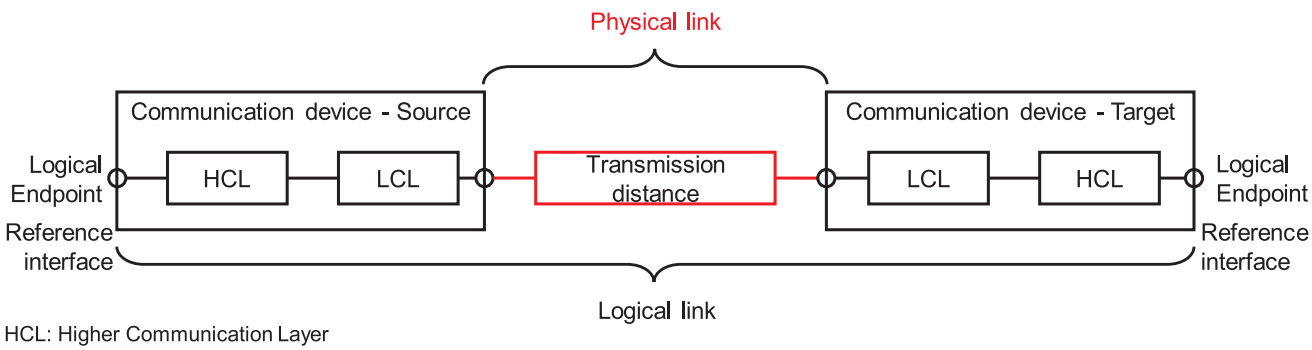


Figure 13: “Physical link” item

In the context of the ZDKI research tender, particular attention is devoted to the transmission distance. The specific influences of the transmission distance on dependability (passive environmental influences) are examined, as is also the aspect of the coexistence of radio applications. On the basis of these research results it will be possible to develop corresponding processes and algorithms for reliable wireless communication.

5.5 Communication system

The communication system as an item represents a quantity of logical links whose message transmissions are implemented by a number of wireless devices via one or more media (Figure 14). The communication system function to be provided consists in transmitting messages for all the logical links in the distributed application. This function is to be performed for a defined period, the operating time of the automation application.

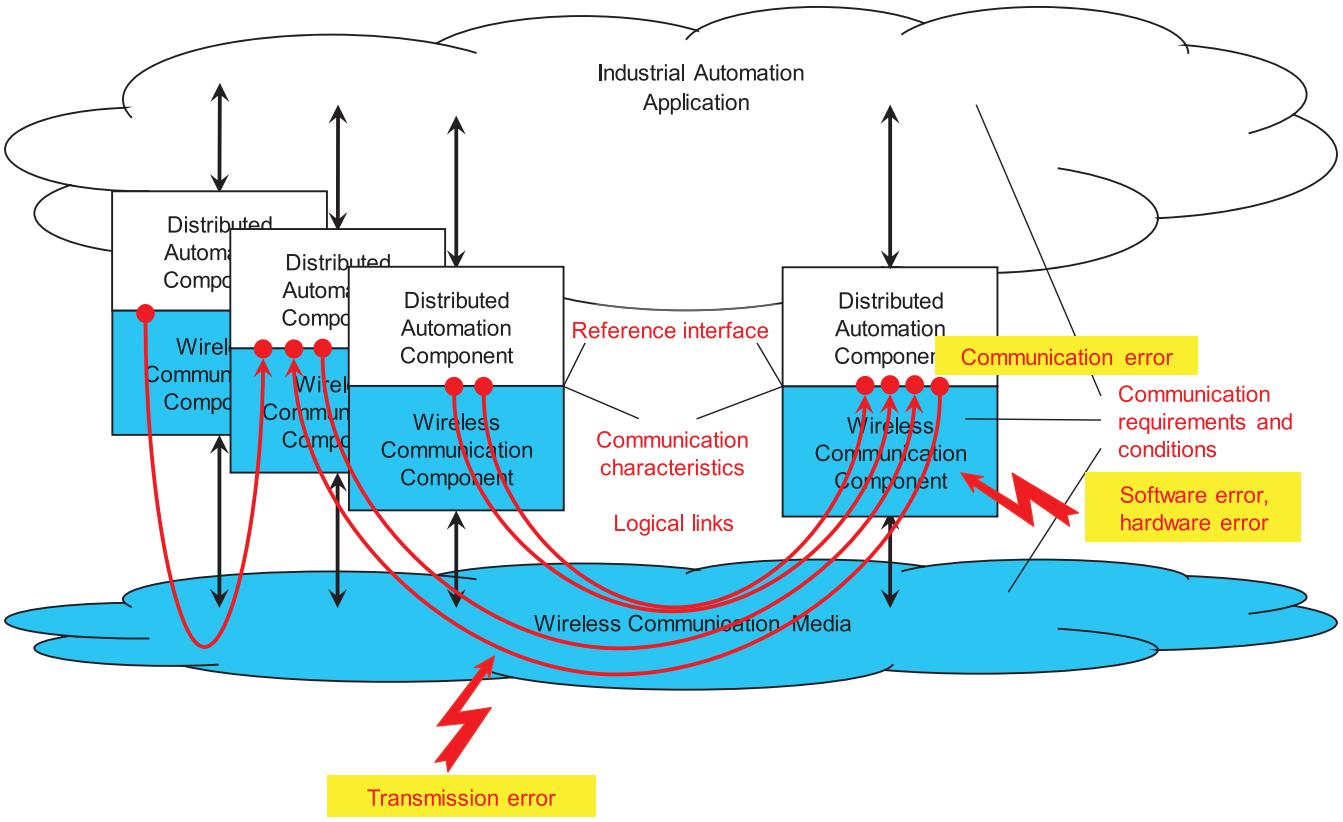


Figure 14: Sources of errors in wireless transmission

The requirements of all the logical links are to be fulfilled. These requirements, and the conditions, can be very different. The functions (services and protocols) for individual logical links can therefore also be different. In spite of these differences, some of the logical links share communication devices and media. That leads to interactions which are not taken into account in connection with the units of consideration which have been discussed up to now. Consequently, the communication system as a whole is suitable as an item for dependability assessment in the examination of system and application aspects.

The errors in message transmission which have already been discussed are also shown in Figure 14. The consideration of the system reveals existing interactions. The cause for a malfunction may be a change in a condition, for instance the occurrence of an interference signal or an increase in the distance between two wireless devices. The reasons for that change manifesting itself as a malfunction can be a lack of robustness, inadequate processes, or defective implementations. The cause may have occurred in one logical link, and nevertheless manifest itself as a communication error in a different one.

In the context of the ZDKI research tender, dependability assessment of the system as a whole forms part of the considerations.

5.6 Conditions influencing function

The quantitative view of the conditions which is necessary for the dependability assessment is not covered by this document. Attention is drawn in this connection to the application-related, wireless device and system-related and environment-related influencing parameters on wireless communication as set out in [19].

5.7 Conclusion

The assessment of dependable wireless communication in industry can be based on consideration of various items. Table 1 summarizes which items are to be subjected to dependability assessment for which aspects of ZDKI. It also indicates which Specialist Group within BZKI is to perform these tasks. The Specialist Group "Applications, Requirements and Validation" is establishing, for instance with this document, the conditions for a uniform approach to dependability assessment within ZDKI. The Specialist Group "Standardization, Interoperability and Best Practices" is working to anchor and harmonize this view of dependability assessment in directives and standards.

Item	Relevance	BZKI Specialist Group
Communication system	System integrators, operators: Discovery of system-related causes of errors Developers: Development of strategies for optimization of dependability	Implementation, Integration and Roadmaps
Logical link	Operators, service providers: Discovery of the causes of errors Developers: Development of strategies for their detection and for avoidance of the effects of errors	Coexistence, Architecture and Interfaces Implementation, Integration and Roadmaps Safety and Security
Communication device	Manufacturers, developers: Development of methods and algorithms for dependable transmission and receipt of messages Developers: Hardware development Manufacturers: Manufacturing process	Radio Air Interface Implementation, Integration and Roadmaps
Physical link	Developers: Characterization of the passive and active environmental influences to be taken into account in the development of concepts and solutions Operators, service providers: Characterization of the passive and active environmental influences to be taken into account in troubleshooting	Coexistence, Architecture and Interfaces Radio Air Interface

Table 1: Items considered for dependability assessment in ZDKI

On application of the performance characteristics, characteristic parameters and probabilistic measures for assessment of dependability described in Section 4, it is to be noted that different features and characteristic parameters are appropriate for different units of consideration. An assignment is made in the following sections.

6 Performance characteristics, characteristic parameters and probabilistic measures for assessment of the dependability of a logical link

6.1 Relevant performance characteristics

The performance characteristics defined in Section 4.2 are listed in Table 2 and evaluated with regard to their relevance to the assessment of a communication link. The characteristics of durability, maintainability und maintenance support performance are ignored in most cases, and the focus of attention is directed at the transmission path. If the transmission path is not functional, this is mostly the result of a fault. After that fault, the functional capability is as a rule (self-)recoverable. It is without question that information security is also a relevant performance characteristic. Functional safety is considered separately in Section 8.

In the following sections, characteristic parameters and their probabilistic measures are discussed with reference to a logical communication link.

IEV Number	Designation EN	Relevant to logical link
192-01-23	Availability	Yes
192-01-24	Reliability	Yes
192-01-25	Recoverability	Yes
192-01-26	Self-recoverability	Yes
192-01-27	Maintainability	No
192-01-29	Maintenance support performance	No
192-01-21	Durability	No
351-57-05	Safety	Yes
–	Information Security	Yes
351-57-06	Functional safety	Yes
715-07-14	Quality of service	Yes

Table 2: Overview of the dependability performance characteristics for a logical link

6.2 Characteristic parameters and their probabilistic measures

6.2.1 Up time

When a logical link is in the up state, a message can be transmitted at any time from the logical end point of the source to the logical end point of the target. The up time begins with the explicit or implicit establishment of a connection, and ends with the failure of the connection or clearing of the connection as a result of a fault. It is to be noted in that context that the measurable up time may deviate from the actual up time. The reason for this is that the up state is determined on the basis of the correctly received messages or incorrectly received or lost messages. Figure 15 shows that the start of an up time period is only detected on the basis of the first successfully received message. The end of the up time period is shown in Figure 15 by the loss of a message. That means that an expected message was not correctly received within the required time limit.

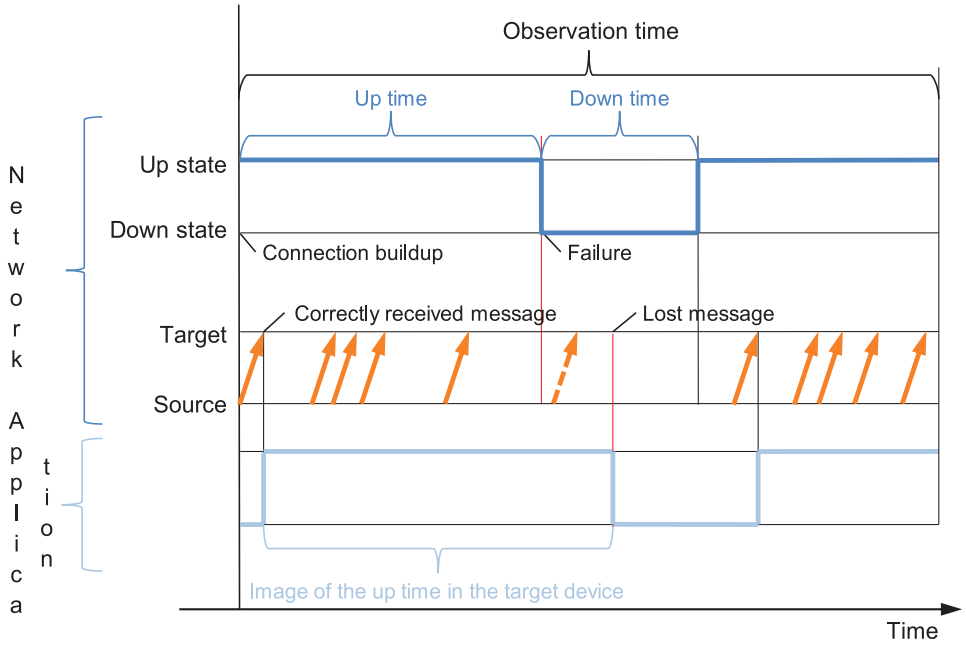


Figure 15: Up time of a logical link

As shown in Figure 15, there may be several up times within an observation time, which may for example be a production period, separated by down time periods.

According to the definition, the expectation value is calculated for analysis of the up time. In the present case, the expectation value is determined by the arithmetical average. The mean up time (MUT) can therefore be calculated as the sum of the up time periods t_U divided by the number of up time periods n, as shown in equation (4).

$$\overline{t_U} = \frac{1}{n}\sum_{i=1}^{n} t_{Ui} = MUT \tag{4}$$

6.2.2 Operating time

A logical link is in operation when it has been set up by the explicit or implicit establishment of a connection. If the link is interrupted by a fault, the operating time is identical to the up time as defined in Section 6.2.1 (see Figure 16). If the connection is intentionally cleared, the logical link no longer exists as an item and requires no further assessment. This means that the idle state shown in Figure 2 and in Figure 4ff. and the associated idle time are not relevant to the logical link.

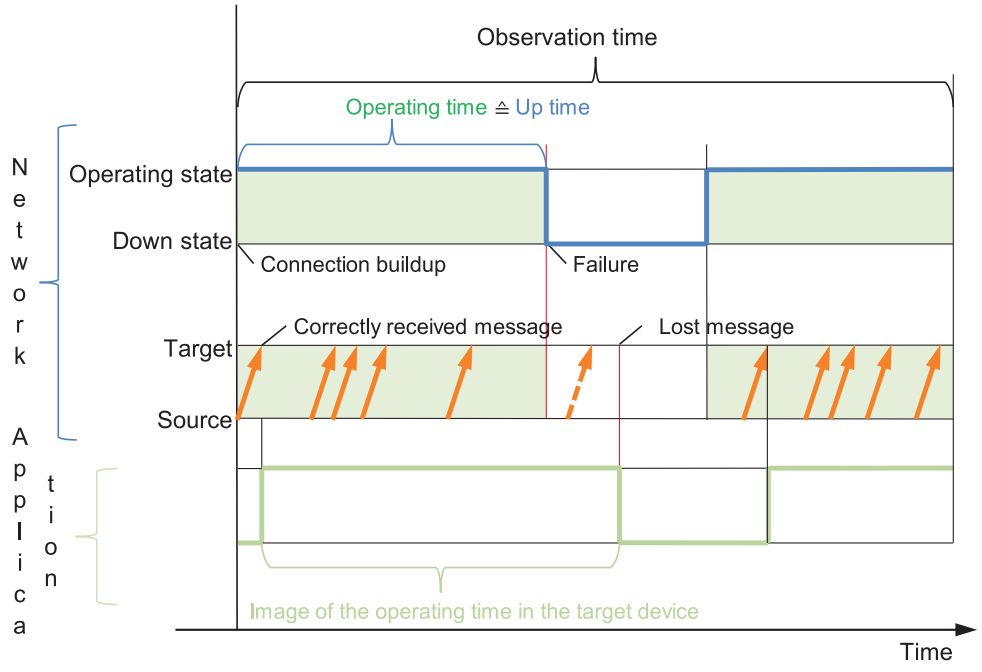


Figure 16: Operating time of a logical link

6.2.3 Down time

The down time starts with the failure of the logical link and ends when it is restored. The failure can be detected on the basis of the first incorrectly received or lost message with the aid of the criteria set out in Section 6.2.12. The image of the down time can however, as shown in Figure 17, deviate from the actual down time. The up state is identified on the basis of receipt of the first correct message.

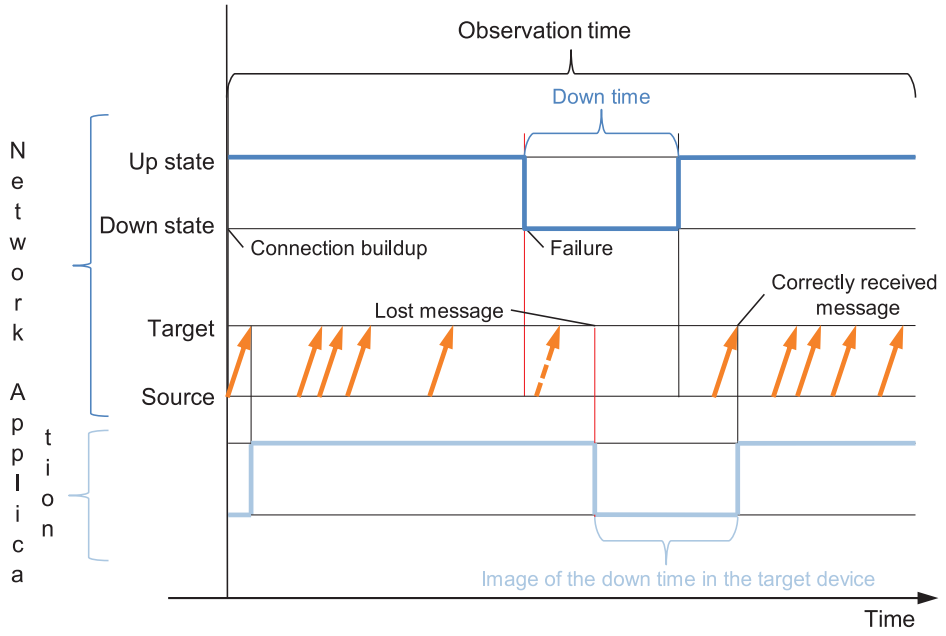


Figure 17: Down time of a logical link

The length of the image of the down time can be used to deduce action to be taken by the application for the protection of humans, machines or products.

According to the definition, the expectation value is calculated for analysis of the down time. In the present case, the expectation value is determined by the arithmetical average. The mean down time (MDT), can therefore be calculated as the sum of the down time periods t_D divided by the number of up time periods n, as shown in equation (5).

$$\overline{t_D} = \frac{1}{n}\sum_{i=1}^{n} t_{Di} = MDT \qquad (5)$$

6.2.4 Operating time to failure

The operating time to failure of a logical link is equivalent to the sum of all operating time periods t_{OP} for which the connection was systematically cleared, including the operating time which was terminated by the first failure (equation (6)).

$$t_{FF} = \sum_{i=1}^{n} t_{OPi} = TTF \text{ where } n = first\ operating\ time\ period\ terminated\ by\ failure \qquad (6)$$

Figure 18 shows two operating time periods, the first of which was terminated by clearing the connection and the second by receipt of an incorrect message.

The operating time to failure is a characteristic parameter of dependability for assessment of the ageing of an item which leads to failure. With reference to the logical link, this concerns the equipment used (e.g. radio device), but not the transmission path.

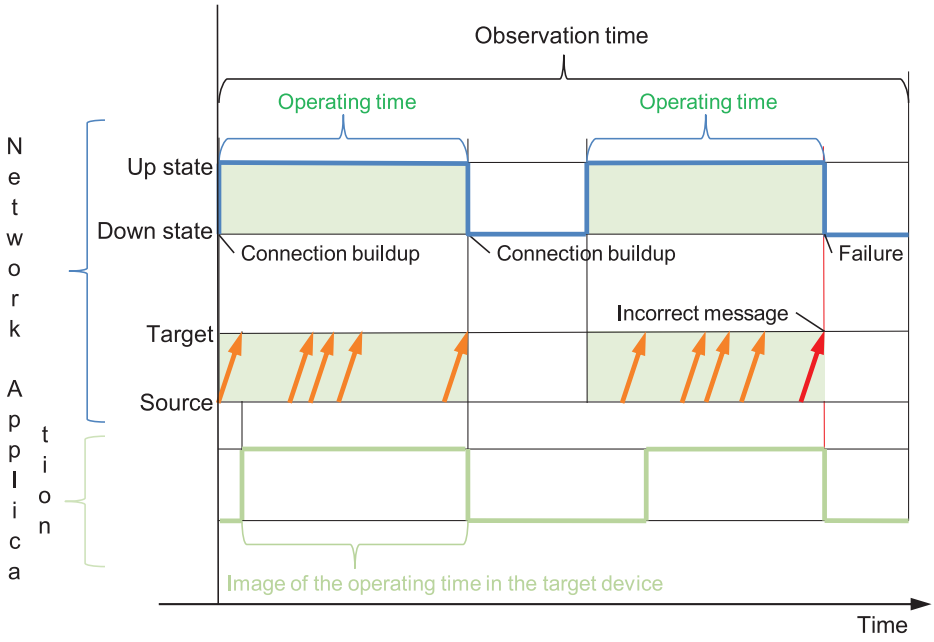


Figure 18: Operating time to failure of a logical link

6.2.5 Time between failures

The time between failures of a logical link results from the duration from one failure to the next. It therefore comprises a down time with at least one incorrect or lost message and an up time or operating time in which at least one message has been transmitted. It can be seen in Figure 19 that there is a difference between the time between failures and the measurable time between failures of the logical link.

According to the definition, the expectation value is calculated for analysis of the time between failures. In a statistical analysis, the expectation value corresponds to the arithmetical average. The individual times between failures can therefore be calculated as the sum of the down time periods t_D and the following up time periods t_U – divided by the number of up time periods n, as shown in equation (7).

$$\bar{t}_G = \frac{1}{n}\sum_{i=1}^{n}(t_{Di} + t_{Ui}) \qquad (7)$$

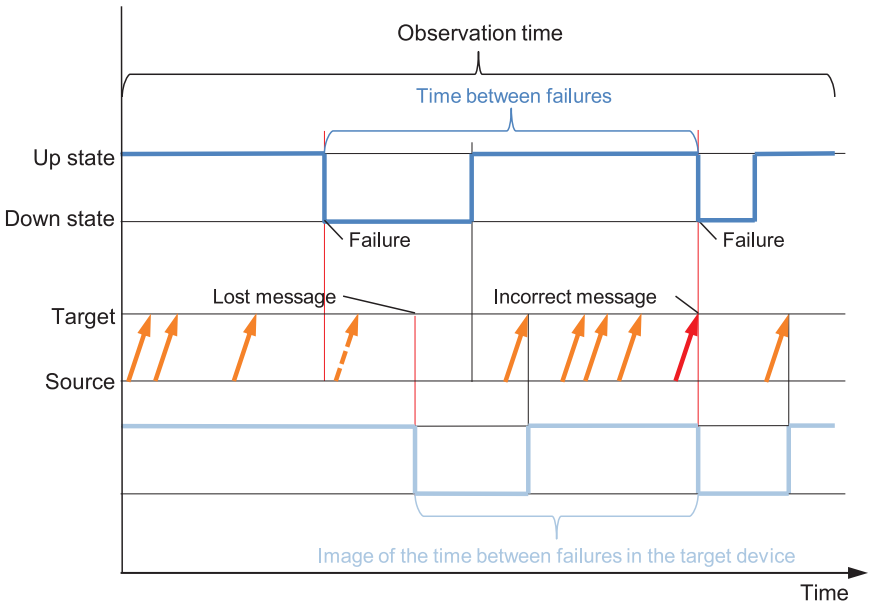


Figure 19: Time between failures of a logical link

6.2.6 Operating time between failures

The operating time between failures of a logical link is the sum of the operating time periods between two successive failures. As shown in equation (8), in the case of a logical link this is also equivalent to the sum of the up time periods between the failures.

$$t_{OP} = \sum_{i=1}^{n} t_{OPi} = \sum_{i=1}^{n} t_{Ui} = T(O)BF \tag{8}$$

$$where\ n = first\ operating\ time\ period\ after\ one\ failure\ which\ is\ terminated\ by\ a\ failure$$

The mean value of the operating time between failures ($MTBF$) is calculated in accordance with equation (9).

$$\bar{t}_{OP} = \frac{1}{n}\sum_{i=1}^{n} t_{OPi} = \frac{1}{n}\sum_{i=1}^{n} t_{Ui} = M(O)TBF \tag{9}$$

6.2.7 Restart time

The restart time is defined as the period between leaving the down state and correct receipt of a message at the target.

The same probabilistic measures are used for the restart time as for the transmission time (see Section 6.2.8), the mode and the P95 percentile value.

6.2.8 Transmission time

The transmission time is a fundamental characteristic parameter which can be used to assess the availability and real time capability of a wireless system. It is interesting in that connection to know how long it takes to transmit a message from the source (e.g. a sensor) to the target (e.g. a controller). A standardized view of this period of time requires precise stipulation of the start and end of that transmission. According to [24], the transmission time is the period from handover of the first indivisible component part of a message, the user data (bit or octet) at the interface between the application and wireless communication device of a source and handover of the last indivisible component part of the same message at the interface between the wireless communication device and application of a target (see Figure 20). The type of interface between the wireless communication device and the application and its characteristics are always to be stated on publication of the characteristic parameter values, as there are no standardized reference interfaces. In figure 20, the arrows are waiting times until transmission or processing. The boxes are time slots for transmission or processing.

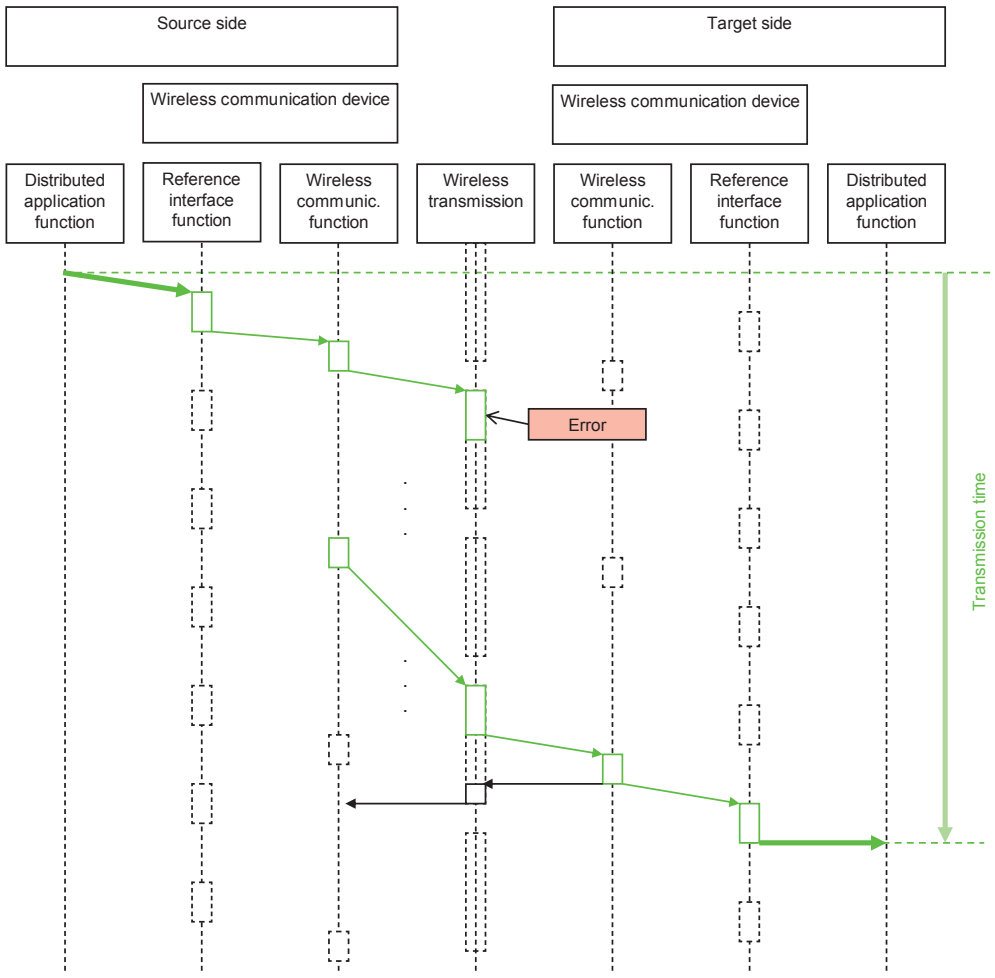


Figure 20: Definition of transmission time

The transmission time is suitable for use as a characteristic parameter of real time capability for applications with non-periodic communication requirements. Independently of the period between two transmissions, the time of provision of the user data at the target device can be assessed. The transmission time is also used in the assessment of dependability.

As shown in Figure 20, the transmission time values fluctuate. One of the reasons for this is there has to be a waiting time for readiness to receive data or for a time slot for access to the medium (shown in each case by a rectangle of dashed lines). The transmission time cannot fall below a minimum, but in most cases adopts a value close to that minimum. The value which occurs most frequently,

the mode, is therefore most suitable for assessment of the centre. The percentile P95, the value for 95% of all transmissions, is an appropriate spread parameter for transmission time. The maximum value for the transmission time can be greater than the mode by several powers of ten, and is therefore unsuitable as a parameter for assessment.

6.2.9 Update time

In the ideal case, the update time is equal to the transfer interval between messages in a logical link. That means that the transmitted user data are received at the reference interface of the target in the same intervals in which they were handed over at the reference interface of the source. The update time is defined as the period from handover of the last indivisible component part of the user data from a source at the reference interface of a target to handover of the last indivisible component part of the user data transmitted directly thereafter from the same source in a logical link. Figure 21 shows that information can in some cases only be passed on at particular times or at particular intervals. This causes the differences between the transfer interval and the update time. In Figure 21, the arrows are waiting times until transmission or processing. The boxes are time slots for transmission or processing.

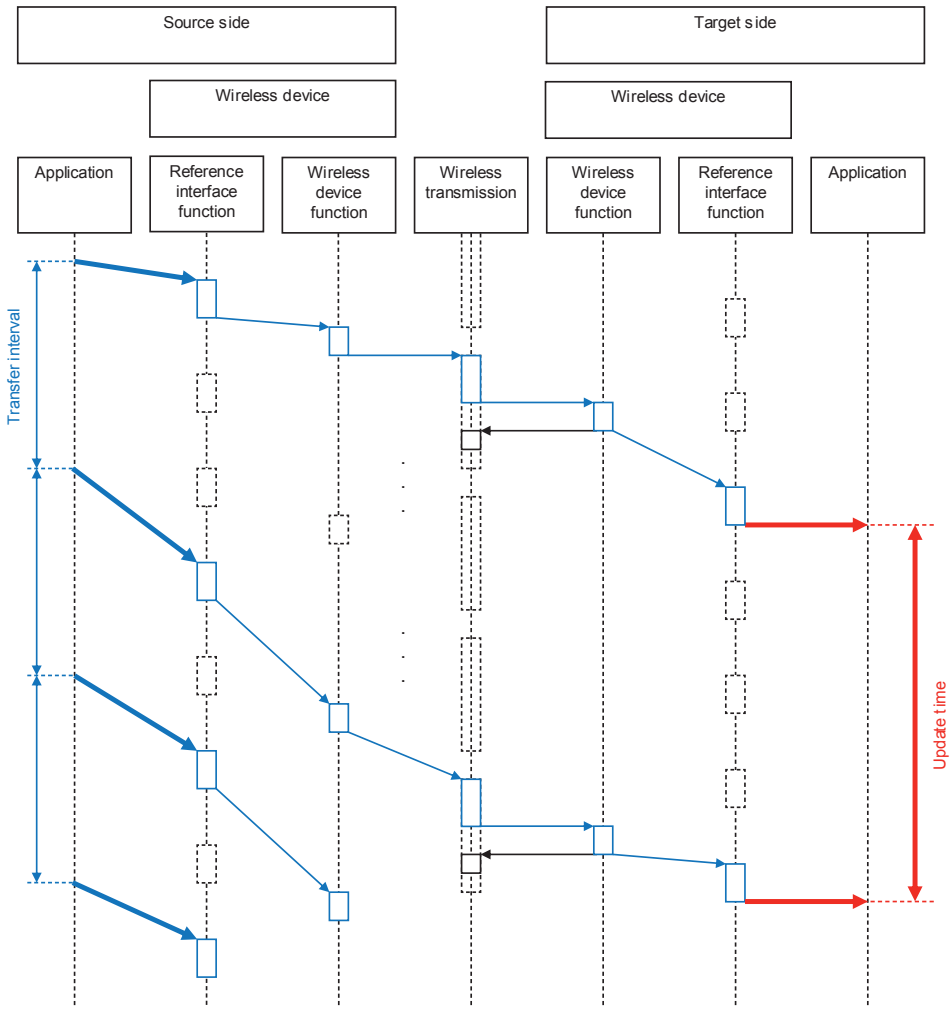


Figure 21: Definition of update time

The update time is especially suitable for assessment of the promptness and determinism of applications with periodic communication requirements [1].

The arithmetical mean and the standard deviation are meaningful probabilistic measures of the update time.

6.2.10 Response time

The response time refers to the transmission of a request message and the corresponding response message. It comprises not only the time for transmission of the messages, but also the time for creation of the response message. The response time is the period from handover of the first indivisible component part of the request message at the reference interface to handover of the last indivisible component part of the corresponding response message at the same reference interface.

The same probabilistic measures are used for the response time as for the transmission time, the mode and the P95 percentile value.

6.2.11 Number of correctly received messages

A message Me_{Rxi} is deemed to have been received when it has been handed over to the application at the reference interface of the target. The number of received messages (N_{RM}) results from the following equation:

$$N_{RM} = \sum_{i=1}^{n} Me_{Rxi} \tag{10}$$

As, however, falsifications of the contents and repetitions of the transmission which are not identified or corrected by the error protection mechanism can occur, the data received are to be checked for these. Promptness is also one of the conditions for a correctly received message.

Consequently, the definition of correctly received messages presented below takes account of the data content (Co), the sequence number (SN), the transmission time $t_T(Me_{Rxi})$ and the addresses (Ad).

$$N_{Rx} = \sum_{i=1}^{n} c(Me_{Rxi}) \tag{11}$$

$$where \begin{cases} c(Me_{Rxi}) = 1, if\ Co(Me_{Rxi}) = Co(Me_{Txi}) \wedge SN(Me_{Rxi}) > SN(Me_{Rxi-1}) \wedge t_T(Me_{Rxi}) \leq T_{Tmax} \\ \wedge\ Ad_{SCR}(Me_{Rxi}) = Ad_{SCR}\ \wedge\ Ad_{TGT}(Me_{Rxi}) = Ad_{TGT} \\ c(Me_{Rxi}) = 0, else \end{cases}$$

N_{Rx} consequently designates the number of correctly received messages, to which the following applies:

- The content of the received data $Co\ (Me_{Rxi})$ agrees in a bit comparison with the content of the transmitted data $Co\ (Me_{Txi})$. There are no bit errors or symbol errors. The correctness of a received message is designated as $c\ (Me_{Rxi})$. A simple CRC test is not sufficient in this respect.
- The sequence number of each received message $SN\ (Me_{Rxi})$ must be greater than the sequence number of the previously received message $SN\ (Me_{Rxi-1})$. Messages which have been overtaken are therefore assessed as false.
- The value of the transmission time $t_T\ (Me_{Rxi})$ must be smaller than a specified limit T_{Tmax}.
- The address of the source $Ad_{SCR}(Me_{Rxi})$ in the message must be identical to the source address of the logical link. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.

- The address of the target $Ad_{TGT}(Me_{Rxi})$ in the message must be identical to the target address of the logical link. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.

Depending on the requirements, the formula may be adapted or further parameters (e.g. update time) added. If a message is correctly received, the system is in the up state.

6.2.12 Number of incorrectly received messages

In the context of this consideration, a received message Me_{Rxi} is deemed false when its transmission time $t_T(Me_{Rxi})$ is greater than a defined maximum T_{Tmax} or when the data content at the target is not identical to that at the source. Furthermore, on transposition of messages, the delayed message is assessed as false, even if has not exceeded the maximum transmission time T_{Tmax}.

Similarly to the case with the correctly received messages, the data content, sequence and the address of a received message are to be taken into account.

The number of false messages (N_{Fx}) therefore results from the following:

$$N_{Fx} = \sum_{i=1}^{n} f(Me_{Rxi}) \tag{12}$$

$$where \begin{cases} f(Me_{Rxi}) = 1, if\ Co(Me_{Rxi}) \neq Co(Me_{Txi}) \vee SN(Me_{Rxi}) \leq SN(Me_{Rxi-1}) \vee t_T(Me_{Rxi}) > T_{Tmax} \\ \vee\ Ad_{SCR}(Me_{Rxi}) \neq Ad_{SCR} \vee Ad_{TGT}(Me_{Rxi}) \neq Ad_{TGT} \\ f(Me_{Rxi}) = 0, else \end{cases}$$

$f(Me_{Rxi})$designates a false message. N_{Fx} designates the number of incorrectly received messages, to which the following applies:

- The content of the received data $Co(Me_{Rxi})$ does not agree in a bit comparison with the content of the transmitted data $Co(Me_{Txi})$. Bit errors or symbol errors have occurred.
- The sequence number of the received message $SN(Me_{Rxi})$ is smaller than or equal to the sequence number of the previously received message $SN(Me_{Rxi-1})$. Messages which have been overtaken are therefore assessed as false.
- The value of the transmission time $t_T(Me_{Rxi})$ is greater than or equal to the specified limit T_{Tmax}.
- The address of the source $Ad_{SCR}(Me_{Rxi})$ in the message is not identical to the source address of the logical link. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.
- The address of the target $Ad_{TGT}(Me_{Rxi})$ in the message is not identical to the target address of the logical link. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.

Depending on the requirements, the formula may be adapted or further parameters (e.g. update time) added.

6.2.13 Number of alien messages received

It is possible for messages which were not intended for the target to be received. They may, for example, originate from an impermissible source, or if the source was permissible the message was intended for a different target. Figure 22 presents a diagram of the receipt of messages of alien origin. A message can be intentionally transmitted to the target (Attacker) or received by chance (Source 2). In both cases it is important for the message to be recognized as false and the false data not included in the interpretation and processing by the application.

With periodic transmission, at least the transfer interval in which the alien message was received counts as a factor for incorrectness. In general, processing of these messages would lead to overwriting of correct messages or blocking of the receipt of correct messages.

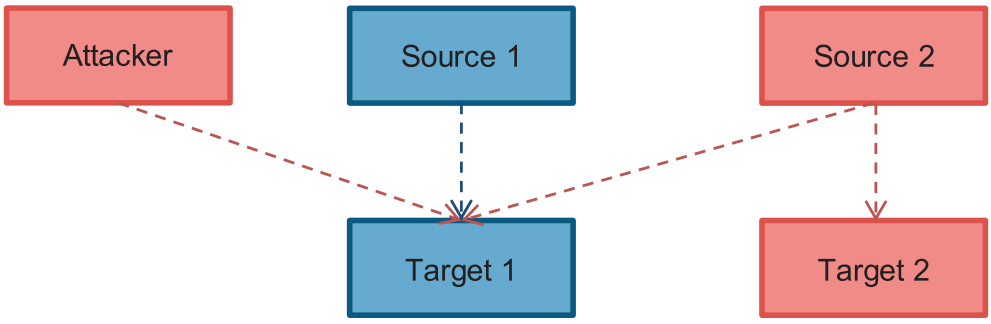


Figure 22: Receipt of a message from an alien source

The number of alien messages received (N_{AN}) is calculated in accordance with the following equation:

$$N_{AN} = \sum_{i=1}^{n} a(Me_{Rxi}) \; where \begin{cases} a(Me_{Rxi}) = 1, \; if \; Ad_{SCR}(Me_{Rxi}) \neq Ad_{SCR} \vee Ad_{TGT}(Me_{Rxi}) \neq Ad_{TGT} \\ a(Me_{Rxi}) = 0, else \end{cases} \quad (13)$$

$a(Me_{Rxi})$ designates the alien origin of a message. N_{AN} consequently designates the number of alien messages received, to which the following applies:

- The address of the source $Ad_{SCR}(Me_{Rxi})$ in the message is not identical with the source address of the logical link.
- The address of the target $Ad_{TGT}(Me_{Rxi})$ in the message is not identical with the target address of the logical link.

6.2.14 Number of lost messages

A message is deemed to be lost when user data handed over at the reference interface of the source are not correctly handed over at the reference interface of the target. It is to be taken into account in that connection that messages of alien origin (N_{AN}) may also be handed over at the reference interface of the target. Account is therefore to be taken in this case of more messages being evaluated than were transmitted by the source of the logical link.

The number of lost messages (N_{LM}) therefore results from the difference between the number of transmitted messages (N_{Tx}) plus the number of received messages of alien origin (N_{AN}) and the messages which were received correctly (N_{Rx}) and incorrectly (N_{Fx}).

$$N_{LM} = N_{Tx} + N_{AN} - (N_{Rx} + N_{Fx}) \quad (14)$$

In order to distinguish better between the different types of messages, an example is presented in Figure 23. S1 is the legitimate source of the logical link, S2 is an illegitimate (alien) source, and T is the target of the logical link. S1 transmits 14 messages ($N_{Tx} = 14$), and S2 transmits 2 messages. The target receives 15 messages.

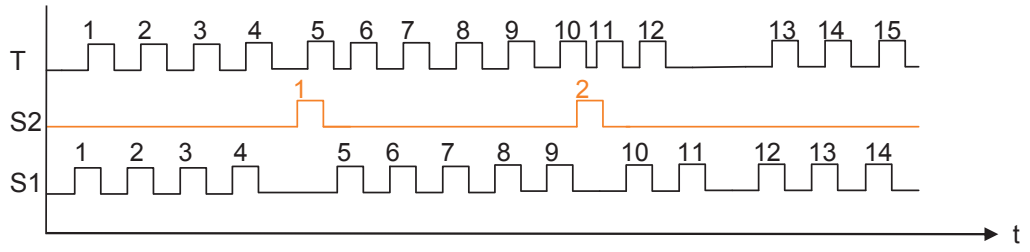


Figure 23: Example: Messages prior to evaluation

The 15 messages received are evaluated. Of these there are, as shown in Figure 24, 10 correctly received messages, 5 incorrectly received messages and 2 received messages of alien origin (source S2). The received messages of alien origin are, as set out in Section 6.2.12, included in the incorrectly received messages.

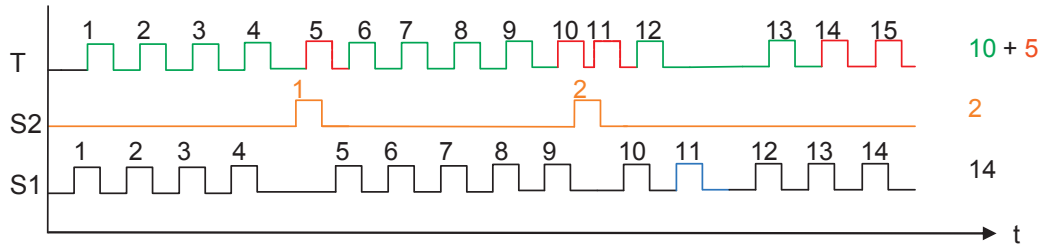


Figure 24: Example: Messages after evaluation

$$N_{LM} = N_{Tx} + N_{AN} - (N_{Rx}) + N_{Fx} = 14 + 2 - (10 + 5) = 1 \quad (15)$$

The example calculation in equation (15) illustrates that the set of received messages of alien origin is a subset of the incorrectly received messages (Figure 25).

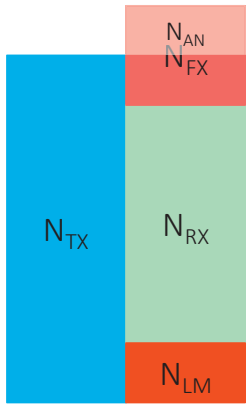


Figure 25: Quantities of transmitted, received and lost messages

6.2.15 Failure rate

The failure rate λ is sometimes also referred to as the error rate. It can be used to assess how often the logical link fails per unit of time.

The mean failure rate, which, as shown in equation (16), corresponds to the reciprocal of the mean operating time between failures, can be used as a probabilistic measure.

$$\overline{\lambda} = \frac{1}{MTBF} \quad (16)$$

6.2.16 Message error ratio

The message error ratio (*MER*) results from the ratio between the incorrectly received messages N_{Fx} and the transmitted messages N_{Tx}.

The message error probability is the probability that the received message, in comparison with the corresponding transmitted message, contains errors and is therefore incorrect.

$$MER = \frac{N_{Fx}}{N_{Tx}} \quad (17)$$

6.2.17 Message loss ratio

The message loss ratio (*MLR*) is, according to [2] IEV 371-08-07, the ratio of the number of lost messages to the total number of messages sent.

$$MLR = \frac{N_{LM}}{N_{Tx}} \quad (18)$$

6.2.18 Ratio of message interference

The ratio of message interference (*RMI*) is the ratio between the number of alien messages received and the total number of transmitted messages.

$$\mathrm{RMI} = \frac{N_{AN}}{N_{Tx}} \quad (19)$$

6.2.19 Residual error rate

The Residual Error Rate (*RER*) is, according to [2] IEV 371-08-05, the ratio of the number of undetected wrong messages to the total number of messages sent.

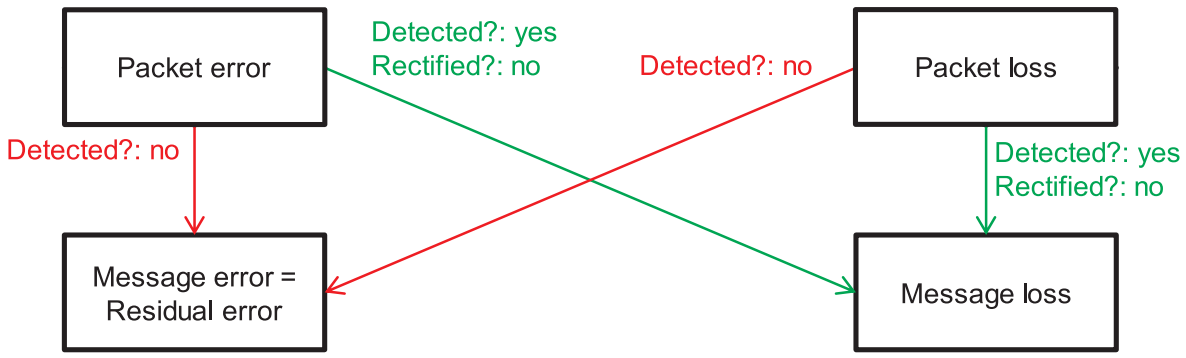


Figure 26: Effects of packet errors and packet losses

Figure 26 shows the possible effects of packet errors and packet losses. Distinctions are made as to whether these are detected and rectified. Four possible cases are distinguished here.

In the first case, the packet error is not detected. This leads to an incorrect message which is forwarded directly to the application. This undetected wrong message is a residual error (cf. definition of residual error rate [2] – IEV 371-08-05, 721-08-56). It therefore follows that in this view the message error rate corresponds to the residual error rate.

In the second case, a packet error is detected, but cannot be rectified. The consequence of this is that the message cannot be assembled. A message loss occurs.

In the third case, a packet loss is not detected. This leads to a message error. The message is incompletely assembled in the upper communication layers and directly passed on to the application. This undetected wrong message is a residual error.

In the fourth case, a packet loss is detected, but cannot be rectified. The consequence of this is that the message cannot be assembled. A message loss occurs.

If packet errors or packet losses are detected and rectified, there is neither a message loss nor a message error. The security and reconstruction mechanisms have successfully intervened and there can be no adverse effects on the message content. For that reason, this case is not represented in the figure.

In [2] IEV 721-08-56 the residual error rate is defined, synonymously with the undetected error rate, as the ratio of the number of bits, unit elements, characters or blocks incorrectly received but undetected or uncorrected by the error control equipment, to the total number of corresponding elements sent.

6.3 Performance characteristics

6.3.1 Availability

According to the definition (Section 4.2.1), the availability (A) is a measure of the ability of an item to be in a state to perform as required within a given period of time. Applied to the function of a logical link, the availability is the ratio of the up time (t_U) to an observation time (t_O):

$$A = \frac{1}{t_O} \sum_{i=1}^{t_O} t_U \qquad (20)$$

Assuming that the source periodically sends a number of transmitted messages (N_{Tx}) with a transfer interval (t_{TI}) in the observation time t_O, and that the wireless system detects each message received in the transfer interval as a correctly received message (N_{Rx}-Section 6.2.11), the availability can be calculated as follows:

$$A = \frac{N_{Rx} t_{TI}}{N_{Tx} t_{TI}} = \frac{N_{Rx}}{N_{Tx}} \quad (21)$$

From the perspective of the application, the characteristic parameters listed and defined in Part 4 of VDI/VDE standard 2185 [1] are relevant to the assessment of dependability.

$$A = \frac{1}{t_O} \sum_{i=1}^{t_O} t_U \quad (22)$$

6.3.2 Reliability

At first sight, there is no difference between the concepts of availability (Section 4.2.1) and reliability (Section 4.2.2). According to the definition of availability, however, reliability is only one of the characteristics of availability. For an assessment of availability, additional consideration is required of those characteristics which describe the avoidance of failures (maintainability) and the restoration of the function (recoverability). That is why a reliable communication link does not necessarily have to have high availability.

In Figure 27 a, the operating time between two failures is on average large compared with Figure 27 b. That means that the reliability is greater in Figure 27 a. A communication link is the more reliable, the more rarely failures occur. The concept of reliability makes no reference to the length of the interruption of the function.

The accumulated reliability is greater in Figure 27 b than in Figure 27 a, and therefore the relationship between the up time and the observation time is better in Figure 27 b. This means that the availability is greater in Figure 27 b. Nevertheless, the operating times between failures (*TBF*–section 4.3.7) in Figure 27 a are longer, as are the failure times.

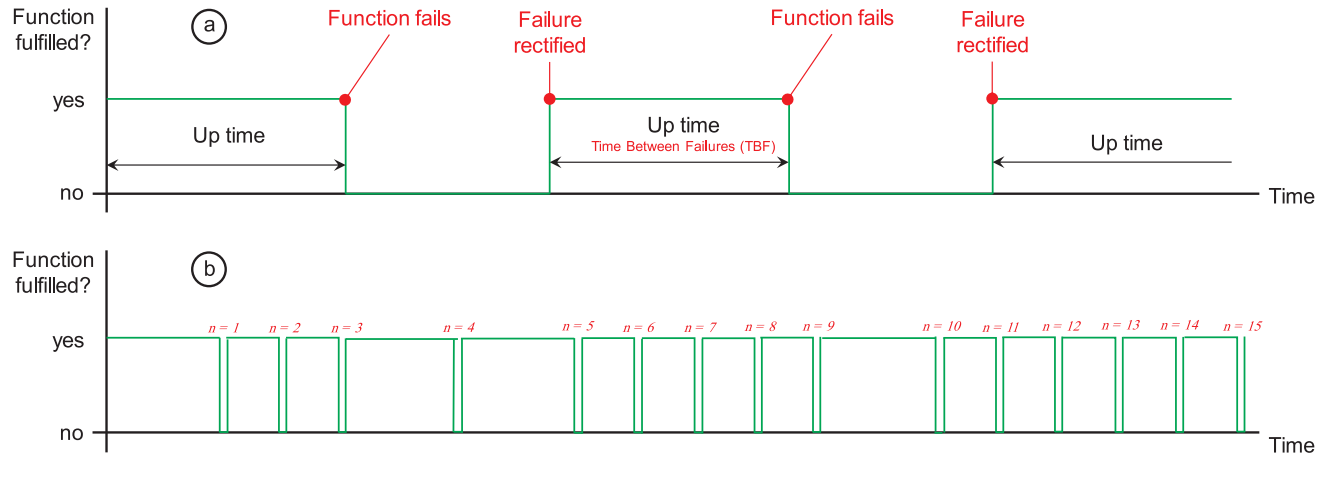


Figure 27: Difference between high reliability (a) and high availability (b)

6.4 Conclusion

Figure 28 presents a breakdown of dependability by the relevant performance characteristics, characteristic parameters and probabilistic measures, based on [18], p.91, and extended to cover wireless communication.

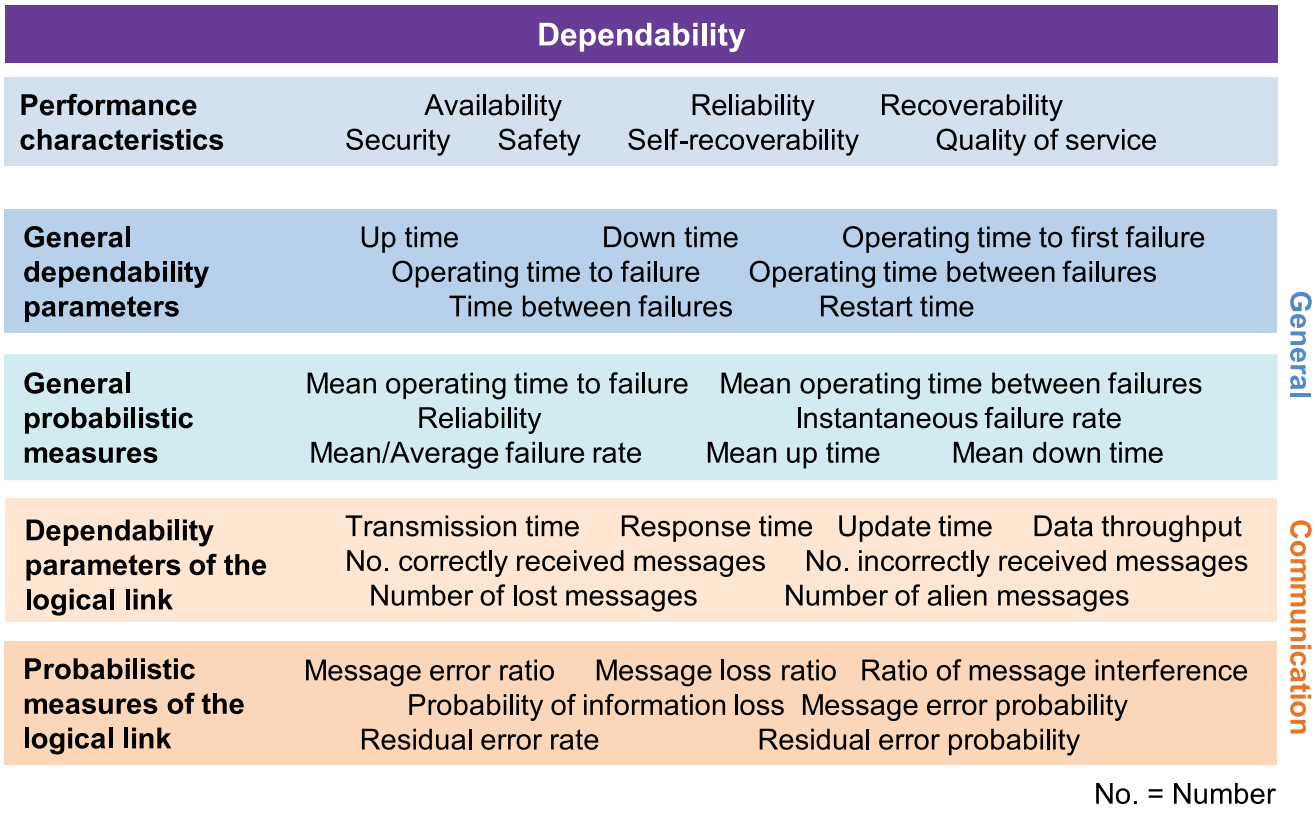


Figure 28: Dependability, performance characteristics, dependability parameters and probabilistic measures

The main focus is on the general dependability parameters – in particular the up time and down time. They are the basis of calculation on the one hand for individual performance characteristics and on the other hand for the general probabilistic measures. The dependability parameters of the logical link, such as the number of correctly or incorrectly received messages, are also assigned by implication to the up time and down time. If a message is correctly received, the system is in the up state. The system remains in the up state for as long as messages are correctly received (up time). If messages are incorrectly received or even lost, the system is in the down state, and remains there until messages are correctly received again. The number of correctly received messages can, then, either refer to the entire observation time (in relation to availability) or to an up time period between failures (in relation to the operating time between failures). These up time periods can themselves be averaged (in relation to the mean operating time between failures). The dependability parameters of the logical link can accordingly also be calculated using the general dependability parameters, performance characteristics and general probabilistic measures. Furthermore, the dependability parameters of the logical link also serve for calculation of a number of probabilistic measures of the logical link, such as the message loss rate, message error rate and ratio of message interference. The probabilities are based on theoretical calculations only, which is why they stand alone and not in relation to other variables.

Within the relevant group, the variables are of course also relative to one another. Among the general dependability parameters, for example, the time between failures (in periodic systems is equal to the up time. Another example is

the restart time, which is part of the down time. The average times (in the group of general probabilistic measures) are calculated from the characteristic parameters which belong to them. The $MTBF$, for example, can then be used to calculate the failure rate λ and that to calculate the reliability function $R(t)$.

7 Performance characteristics, characteristic parameters and probabilistic measures for assessment of the dependability of the other items

7.1 General

The observations from Section 6 can also be made for the other items discussed in Section 5. In the following, these are limited to a few aspects only.

7.2 Communication device

7.2.1 General

The performance characteristics for dependability of a communication device are assessed in Table 3.

IEV Number	Designation EN	Relevant to communication device
192-01-23	Availability	Yes
192-01-24	Reliability	Yes
192-01-25	Recoverability	Yes
192-01-26	Self-recoverability	Yes
192-01-27	Maintainability	Yes
192-01-29	Maintenance support performance	Yes
192-01-21	Durability	Yes
351-57-05	Safety	Yes
–	Information Security	Yes
351-57-06	Functional safety	Yes
715-07-14	Quality of service	Yes

Table 3: Overview of the dependability performance characteristics of a communication device

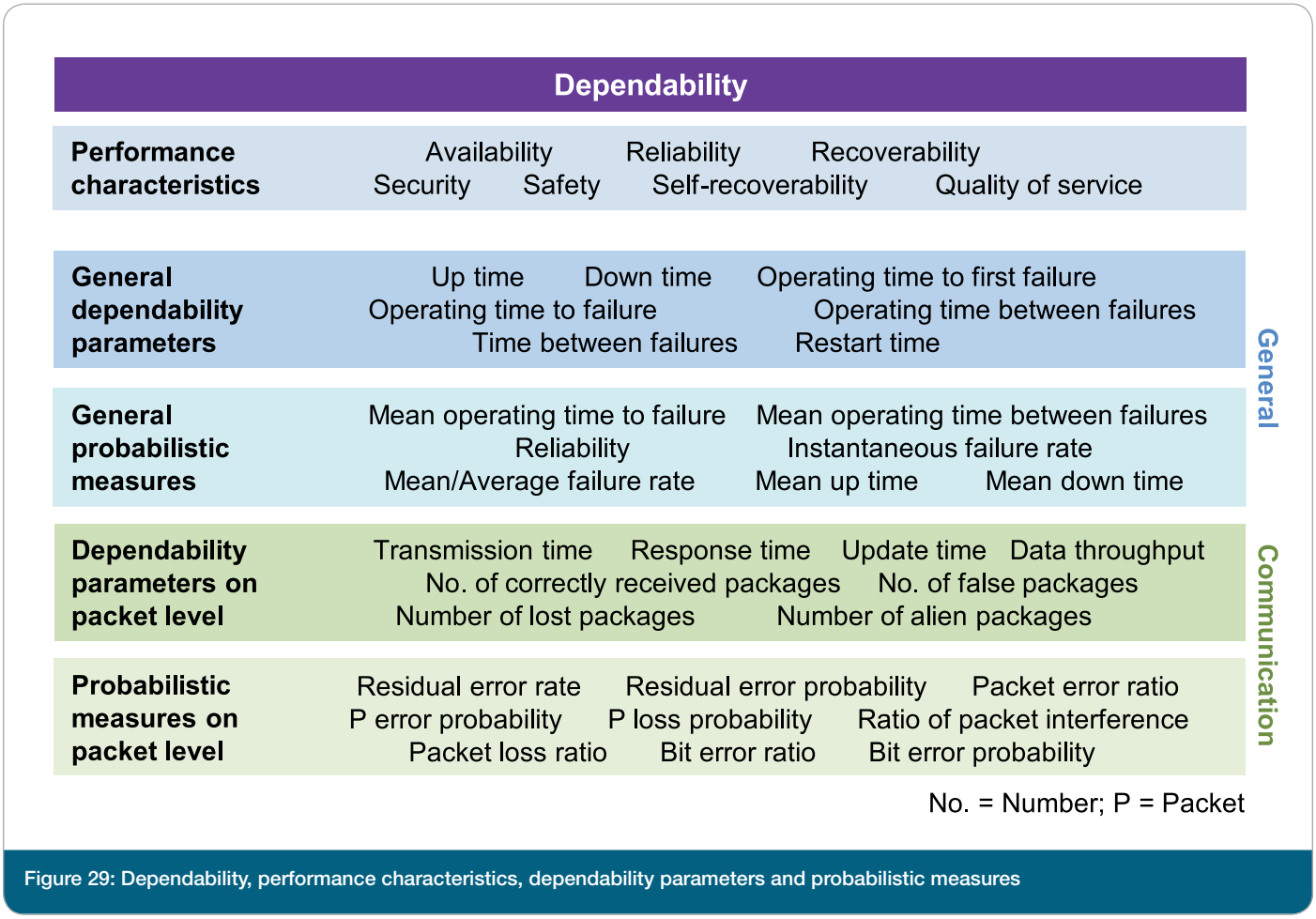


Figure 29: Dependability, performance characteristics, dependability parameters and probabilistic measures

On the level of communication devices of the lower communication layers, we speak of the transmission of packets and not, as in the case of the logical link, of messages. The corresponding characteristic parameters and probabilistic measures are presented for the sake of completeness in Figure 29, but are not in the focus of attention for the assessment.

In addition, there are characteristic parameters which provide information on maintenance, maintenance support performance and on the performance of hardware and software. These parameters are also not in the focus of attention, and will not therefore be discussed further here.

7.2.2 Number of correctly received packets

A packet P_{Ri} is deemed received when it has been handed over at the reference interface of the target to higher communication layers. The number of received packets (N_{RP}) results from the following equation:

$$N_{RP} = \sum_{i=1}^{n} P_{Ri} \tag{23}$$

As, however, falsifications and repetitions of the transmission which are not identified or corrected by the error protection mechanisms of the wireless system can occur, the data received are to be checked for these. Promptness is also one of the conditions for a correctly received packet. Consequently, the definition of correctly received packets presented below takes account of the data content (Co), the sequence number (SN), the transmission time t_T (P_{Ri}) and the addresses of the devices (Ad).

$$N_{RCP} = \sum_{i=1}^{n} c(P_{Ri}) \tag{24}$$

$$where \begin{cases} c(P_{Ri}) = 1, if\ Co(P_{Ri}) = Co(P_{Ri}) \wedge SN(P_{Ri}) > SN(P_{Ri-1}) \wedge t_T(P_{Ri}) \leq T_{Tmax} \\ \wedge\ Ad_{SCR}(P_{Ri}) \in A\ \wedge\ Ad_{TGT}(P_{Ri}) \in B \\ c(P_{Ri}) = 0, else \end{cases}$$

N_{RCP} consequently designates the number of correctly received packets, to which the following applies:

- The content of the received data $Co(P_{Ri})$ agrees in a bit comparison with the content of the transmitted data $Co(P_{Ri})$. There are no bit errors or symbol errors. The correctness of a received packet is designated as $c(P_{Ri})$. A simple CRC test is not sufficient in this respect.
- The sequence number of each received packet $SN(P_{Ri})$ must be greater than the sequence number of the previously received packet $SN(P_{Ri-1})$. Packets which have been overtaken are therefore assessed as lost.
- The value of the transmission time $t_T(P_{Ri})$ must be smaller than a specified limit T_{Tmax}.
- The address of the source $Ad_{SCR}(P_{Ri})$ in the packet must be an integral part of set A of the permitted sources. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request
- The address of the target $Ad_{TGT}(P_{Ri})$ in the packet must be an integral part of set B of the permitted targets. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.

This represents the general case of several targets and sources. Depending on the requirements, the formula may be adapted or further parameters (update time or jitter) added.

7.2.3 Number of incorrectly received packets

In the context of this consideration, a received packet P_{Ri} is deemed false when its transmission time $t_T(P_{Ri})$ is greater than a defined maximum T_{Tmax} or when the data content at the target is not identical to that at the source. Furthermore, on transposition of packets, the delayed packet is assessed as false, even if has not exceeded the maximum transmission time T_{Tmax}. Similarly to the case with the correctly received packets, the data content, sequence and the device address of a received packet are to be taken into account.

The number of false packets (N_{FP}) therefore results from the following:

$$N_{RFP} = \sum_{i=1}^{n} f(P_{Ri}) \tag{25}$$

$$where \begin{cases} f(P_{Ri}) = 1, if\ Co(P_{Ri}) \neq Co(P_{Ri}) \vee SN(P_{Ri}) \leq SN(P_{Ri-1}) \vee t_T(P_{Ri}) > T_{Tmax} \\ \vee\ Ad_{SCR}(P_{Ri}) \notin A \vee Ad_{TGT}(P_{Ri}) \notin B \\ f(P_{Ri}) = 0, else \end{cases}$$

N_{RFP} designates the number of incorrectly received packets, to which the following applies:

- The content of the received data $Co(P_{Ri})$ does not agree in a bit comparison with the content of the transmitted data $Co(P_{Ri})$. Bit errors or symbol errors have occurred.
- The sequence number of the received packet $SN(P_{Ri})$ is smaller than or equal to the sequence number of the previously received packet $SN(P_{Ri-1})$. Packets which have been overtaken are therefore assessed as false.
- The value of the transmission time $t_T(P_{Ri})$ is greater than or equal to the specified limit T_{Tmax}.
- The address of the source $Ad_{SCR}(P_{Ri})$ in the packet is not an integral part of set A of the permitted sources. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.
- The address of the target $Ad_{TGT}(P_{Ri})$ in the packet is not an integral part of set B of the permitted targets. The parameters by which the address is defined (node addresses, port, end point) depend on the relevant request.

This represents the general case of several targets and sources. Depending on the requirements, the formula may be adapted or further parameters (update time or jitter) added.

7.2.4 Number of alien packets received

It is possible for packets which were not intended for the target to be received. They may, for example, originate from an impermissible source, or if the source was permissible the packet was intended for a different target. A packet can be intentionally transmitted to the target or received by chance. In both cases it is important for the packet to be recognized as false and not accepted, so that the false data are not interpreted and processed.

The number of alien packets received (N_{ANP}) is calculated as follows:

$$N_{ANP} = \sum_{i=1}^{n} a(P_{Ri}) \; where \begin{cases} a(P_{Ri}) = 1, if \; Ad_{SCR}(P_{Ri}) \notin A \vee Ad_{TGT}(P_{Ri}) \notin B \\ a(P_{Ri}) = 0, else \end{cases} \quad (26)$$

$a(P_{Ri})$ designates the alien origin of a packet. N_{ANP} consequently designates the number of alien packets received, to which the following applies:

- The address of the source $Ad_{SCR}(P_{Ri})$ in the packet is not part of set A of the permitted sources.
- The address of the target $Ad_{TGT}(P_{Ri})$ in the packet is not part of set B of the permitted targets.

7.2.5 Number of lost packets

A message is deemed to be lost when user data handed over at the reference interface of the source are not handed over at the reference interface of the target. The number of lost packets (N_{LP}) results from the difference between the number of transmitted packets (N_{TP}) plus the number of received packets of alien origin (N_{ANP}) and the number of correctly and incorrectly received packets (N_{RCP}, N_{RFP}).

$$N_{LP} = N_{TP} - N_{RCP} - N_{RFP} + N_{ANP} \quad (27)$$

In a simplified case in which there is only one source and one target, the following applies:

$$N_{LP} = N_{TP} - N_{RP} \quad (28)$$

The number of lost packets N_{LP} results from the transmitted packets (N_{TP}) uand the received packets N_{RP}.

7.2.6 Packet error ratio and packet error probability

The packet error probability, which can be calculated as follows from the bit error probability (p) and the packet length (L) is sometimes used as the criterion for the quality of a transmission path.

$$p_E = 1 - (1 - p)^L \tag{29}$$

In practice, the packet error probability and packet error ratio (PER) and the bit error probability and bit error rate (BER) are frequently taken to be the same. Fundamentally, however, the probabilities are theoretical values, while the rates can be determined by measurements.

The packet error ratio results from dividing the number of incorrectly received (false) packet N_{RFP} by the number of transmitted packets N_{TP}.

$$\mathrm{PER} = \frac{N_{RFP}}{N_{TP}} \tag{30}$$

In contrast to the rates, the probabilities describe the likelihood of a bit error or packet error occurring, calculated by theoretical considerations. These calculations of packet error and bit error probabilities are as a rule only possible for idealized scenarios. They are frequently used to determine the limits to the efficiency of communication systems.

7.2.7 Packet loss ratio

The packet loss ratio (PLR) is the ratio between the number of lost packets and the total number of transmitted packets.

$$\mathrm{PLR} = \frac{N_{LM}}{N_{Tx}} \tag{31}$$

7.2.8 Ratio of packet interference

The ratio of packet interference (RPI) s the ratio between the number of alien packets received and the total number of transmitted packets.

The ratio of packet interference is a measure of the stress placed on a target device by the receipt of alien packets. Impairments are deduced from this.

$$\mathrm{RPI} = \frac{N_{AP}}{N_{TP}} \tag{32}$$

7.3 Physical link

The performance characteristics for dependability of a physical link are assessed in Table 4

IEV Number	Designation EN	Relevant to physical link
192-01-23	Availability	Yes
192-01-24	Reliability	Yes
192-01-25	Recoverability	Yes
192-01-26	Self-recoverability	Yes
192-01-27	Maintainability	No
192-01-29	Maintenance support performance	No
192-01-21	Durability	No
351-57-05	Safety	Yes
–	Information Security	Yes
351-57-06	Functional safety	No
715-07-14	Quality of service	Yes

Table 4: Overview of the dependability performance characteristics of a physical link

The relevant characteristic parameters for the physical link include, for example, the bit error rate, bit error probability and symbol error probability. These characteristic parameters are not relevant to the logical link, as bit errors are rectified by a mechanism when the bits are grouped together in a packet. These mechanisms are intended to ensure that the packets can be correctly received in spite of bit errors. The definitions are presented below for the sake of completeness.

Bit error rate (*BER*) ([2] – IEV 371-08-01)
"The ratio of the number of bits received inverted to the total number of bits sent."

Bit error ratio ([2] – IEV 704-18-04)
"The error ratio for a binary signal."

Bit error probability ([2] – IEV 371-08-02)
"The probability that a received bit will be inverted with respect to the corresponding bit sent."

7.4 Communication system

The communication system comprises several logical links which may have different requirements for the individual characteristic parameters such as the transmission time or data throughput. The important characteristic parameters of the communication system are the up times and down times of the system, the survivability of the system (single, double, n-times) [25] and in general the relationships between component and system states with regard to redundancy.

Performance characteristics (Table 5) such as availability and recoverability of the communication system are of great relevance, as in the case of the logical link. An overall assessment of the functional safety of communication systems is not possible to date.

IEV Number	Designation EN	Relevant to communication system
192-01-23	Availability	Yes
192-01-24	Reliability	Yes
192-01-25	Recoverability	Yes
192-01-26	Self-recoverability	Yes
192-01-27	Maintainability	Yes
192-01-29	Maintenance support performance	Yes
192-01-21	Durability	Yes
351-57-05	Safety	Yes
–	Information Security	Yes
351-57-06	Functional safety	No
715-07-14	Quality of service	Yes

Table 5: Overview of the dependability performance characteristics of a communication system

8 Considerations of dependability based on the example of functional safety

8.1 Motivation

The dependability of industrial communication systems is considered here in particular for functionally safe applications. Probabilistic measures described above are used for assessment and verification of dependability. This field is therefore an example of the practical application of those measures.

8.2 Principles for safety communication systems

Safety communication systems are nowadays mostly based on the black channel principle, in which a safety protocol is integrated between the safety application and a non-safe communication channel. This safety communication layer has the same safety level as the safety-related system and detects or controls the transmission errors in the communication channel below (black channel). Table 6 from [26] presents measures for detection of communication errors which are integrated in the safety communication layer. Each safety measure can lead to the detection of one or more errors.

Error	Measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross cheking	Different data integrity assurance systems
Corruption					x	x	For serial buses only	
Unintended repetition	x	x					x	
Incorrect sequence	x	x					x	
Loss	x				x		x	
Unacceptable delay		x	x					
Insertion	x			x	x		x	
Masquerade				x	x			x
Incorrect addressing				x				

Table 6: Overview of the effectiveness of the various measures on the possible errors [26]

With the use of this safety communication layer, therefore, complex communication processes such as Ethernet and wireless-based protocols, and also network transitions between sub-systems and backplane buses, without it being necessary to demonstrate compliance with safety standards such as IEC 61508. However, the measures already included in the communication channel (CRC, time monitoring, etc.) are not taken into account in the safety assessment. The additional, possibly redundant, measures go hand in hand with disadvantages in the time-related behaviour of the communication link, which can be reduced or avoided on application of the so-called white channel principle. In contrast to the black channel principle, the complete communication channel (hardware, software and network components) has to be designed, implemented and tested in accordance with IEC 61508, wherever safety functions are directly implemented in the communication channel or the measures involved are to be taken into account in the safety assessment [27]. The probabilistic measures described above can help in the assessment and testing.

8.3 Safety Integrity Level

Failure probabilities and/or failure rates can be used for assessment of the dependability of the system as a whole. Depending on those failure probabilities, the systems can achieve different Safety Integrity Levels, as shown in Table 7.

Safety Integrity Level (*SIL*)	High demand or continuous operating mode (average frequency of dangerous failure per hour (*PFH*))
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Table 7: Safety Integrity Level: Failure limits for a safety function which is operated in high demand or continuous mode [28]

It is to be noted in that context that a logical link in the safe communication channel should not require more than 1% of the maximum values of PFH_d of the target *SIL* (see figure 30).

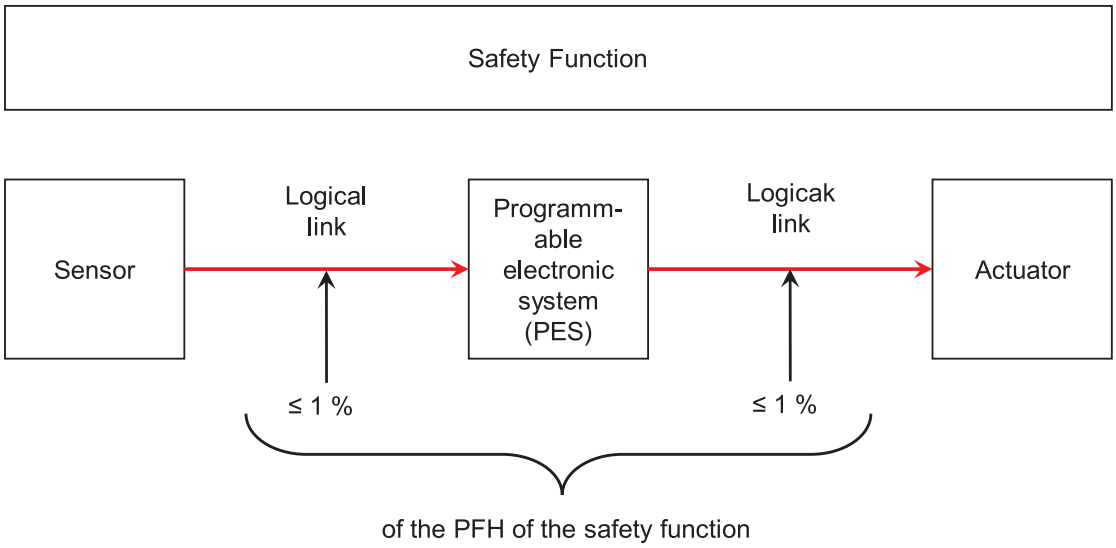


Figure 30: Functionally safe communication as part of a safety function

If, for example, the safety function is to reach *SIL2* with a PFH_d of 10^{-6}, the failure rate at the end points of the logical link may not exceed 10^{-8}.

8.4 Average frequency of a dangerous failure per hour

Average frequency of a dangerous failure per hour (*PFH*) (IEC 61508-4 3.6.19 [29])

Probability of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function for a given period. [...]

Note 3 to entry: When the E/E/EP safety-related system is the last safety layer, *PFH* should be calculated from its failure probability $F(T)=1-R(t)$ (see Failure rate). f it is not the last safety-related system, the should be calculated from the non-availability $U(t)$ […]. Approximate *PFH*'s are given by $\frac{F(T)}{T}$ and $\frac{1}{MFFT}$ oder $\frac{1}{MTBF}$ […].

9 Summary

There is no simple formula for quantitative determination of dependability.

In principle, the definitions of dependability can be divided into two groups:

1. Dependability is defined as a generic term, encompassing availability, reliability, maintainability, etc.
2. Dependability is regarded as reliability of function – the function is performed for a defined time.

It is one of the aims of this document to group together and classify the various terminologies involved with dependability, so as to facilitate understanding and communication between reliability engineers, communication engineers and users.

Possible types of communication errors are discussed and measures for their detection identified.

The performance characteristics and characteristic parameters help in assessing both parts of the system such as the communication path and the system as a whole including hardware and software components in quantitative terms.

One indispensable factor for assessment of dependability is availability. This includes reliability, and can be calculated from the up time and down time.

A further important parameter is the mean operating time between failures (*MTBF*). By calculating the *MTBF*, it is possible under constant demands and conditions to determine what effect specific safety measures in the communication links will have. This factor can therefore provide valuable information for the development or installation of wireless systems. An *MTBF* determined during operation can be an indicator of changes to the dependability of the transmission, and can therefore be used for status messages or diagnosis purposes. The failure rate is the reciprocal of the *MTBF* and can be used for assessment of the system as a whole when account is taken of the failure rates of further components.

For assessment of dependability in wireless communication, it is important to define the area of consideration and the type of transmission, packets or messages to which (application-related) reference is made. This document focuses on the logical link between two applications as the area of consideration, and thus on transmission of the message. With the transmission of packets, there is a broad range of mechanisms for rectification of errors and losses, such that the message can be correctly received by the application irrespectively of those errors and losses. Loss of a packet is not necessarily the same as loss of the message.

With regard to the message, the characteristic parameters and probabilistic measures can adopt different priorities – always in relation to the requirements of the system concerned. The established variables are the following:

- Transmission time
- Update time
- Response time
- Number of lost messages
- Message loss ratio
- Residual error rate

The residual error rate plays an important role, as it illustrates the relationship between undetected false messages and the total number of transmitted messages. It is therefore an indicator of how well the mechanisms for correct and safe data transmission are functioning.

Mathematical relationships between the characteristic parameters and parameters for assessment of dependability are explored.

It must be pointed out that the assessment of dependability is not merely useful for the planning of functional units (software, hardware, links and systems). A standardized dependability assessment is the basis for the development of processes which detect changes to dependability during operation and react in good time before a failure occurs. Such resilient communication systems and their functional components will require further research initiatives (see also [30]).

10 Sources

[1] VDI/VDE: Funkgestützte Kommunikation in der Automatisierungstechnik (Radio based communication in industrial automation), VDI/VDE Richtlinie 2185, Blatt 1 / Part 1

[2] DKE: DKE Wörterbuch, dictionary website, https://www2.dke.de/de/Online-Service/DKE-IEV/Seiten/IEV-Woerterbuch.aspx, 2016

[3] Industialradio: Glossary: http://industrialradio.de/Menu/Home/Glossar, 2016

[4] http://wirtschaftslexikon.gabler.de/Definition/quote.html, May 2017

[5] Plakos: Zuverlässigkeit - Bedeutung, Definition und Sprüche, Internet, https://zuverlaessigkeit.plakos.de/, 2016

[6] VDI: Zuverlässigkeitsmanagement (Reliability Management), VDI 4003, July 2005

[7] DIN: Zuverlässigkeit; Begriffe (Dependability, concepts), DIN 40 041, Dec. 1990

[8] J. Franz: Vorlesungen über Zuverlässigkeit und Statistik bei reparierbaren Systemen, Dresdner Schriften zur Mathematischen Stochastik, Technische Universität Dresden, 2016

[9] H. Bartsch: Definition Technische Zuverlässigkeit, Internet, http://www.heinz-bartsch.de/TZ-1.PDF, 2016

[10] IEC: International electrotechnical vocabulary - Part 192: Dependability, 2015

[11] EN: Industrielle Kommunikationsnetze - Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Profilfestlegungen (Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and Profile definitions), IEC 61784-3:2016

[12] Wikipedia: Zuverlässigkeit (Telekommunikation), web page, https://de.wikipedia.org/wiki/Zuverl%C3%A4ssigkeit_(Telekommunikation), 2016

[13] ITU-R, Rec. ITU-R P.842-2: Computation of reliability and compatibility of HF radio systems

[14] ITU-T, Series Y: Global Information Infrastructure terminology: Terms and definitions, Y101, 03/2000

[15] ETSI EG 202 009-1: User Group; Quality of telecom services; Part 1, 01/2007

[16] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers - Critical Communications; Stage 1 (Release 14), June 2016

[17] DIN EN 61703:2002; Mathematische Ausdrücke für Begriffe der Funktionsfähigkeit, Verfügbarkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft

[18] IEC 61703:2016; Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[19] ITU-T E.800 ITU-T (09/08) “Definitions of terms related to quality of service”

[20] Lutz Rauchhaupt, Elke Hintze, André Gnad: Über die Bewertung der Zuverlässigkeit industrieller Funklösungen – Teil 1 Theoretische Grundlagen, atp 49 Heft 3, S. 38, 2007

[21] L. Rauchhaupt, D. Schulze, A. Gnad: Anforderungsprofile im ZDKI Aspekte der Zuverlässigkeitsbewertung in ZDKI, Fachgruppe 1 “Anwendungen, Anforderungen und Validierung” im BMBF-Förderprogramm “IKT 2020 – Zuverlässige drahtlose Kommunikation in der Industrie” (BZKI), 2016

[22] IEC: Industrial communication networks - High availability automation networks - Part 1: General concepts and calculation methods, IEC 62439-1

[23] IEC: Methodology for communication network dependability assessment and assurance, IEC 62673, 2013

[24] IEC: Industrial communication networks – Wireless communication networks – Part 2: Coexistence management, IEC 62657-2

[25] D. Reichelt, F. Rothlauf; Verfahren zur Berechnung der Zuverlässigkeit von Kommunikationsnetzwerken – Eine Studie zu exakten und approximativen Verfahren; 2004; Working Paper

[26] IEC: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions, IEC 61784-3

[27] E. Hintze, L. Rauchhaupt: Funktionale Sicherheit im Kontext von IIoT, Computer & Automation Sonderheft Safety & Security, S3-2016, S. 26ff, Juli 2016

[28] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements, IEC 61508-1 Ed. 2.0, 2010

[29] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations, IEC 61508-4 Ed. 2.0, 2010

[30] VDE Positionspapier “Resiliente Netze mit Funkzugang” 20.03.2017

[31] Peterson, W. Wesley: Error-Correction Codes, 2nd Edition 1981, MIT-Press

[32] DIN: Internationales Elektrotechnisches Wörterbuch - Teil 351: Leittechnik, DIN IEC 60050

[33] DIN: Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS); Deutsche Fassung EN 50126:1999

[34] IEC: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, IEC 61508-6 Ed. 2.0, 2010

[35] VDI/VDE: Funkgestützte Kommunikation in der Automatisierungstechnik, VDI/VDE Richtlinie 2185, Blatt 2

[36] H.–T. Hannen: Beitrag zur Analyse sicherer Kommunikationsprotokolle im industriellen Einsatz, Dissertation, Universität Kassel, 2012

[37] P.-W. Gräber, Automatisierungstechnik in der Wasserwirtschaft, 2009, Vorlesungsskript Kapitel 6 Messfehler

[38] Grundlagen der Statistik; http://www.statistics4u.info/fundstat_germ/ee_precision_accuracy.html Januar 2017

[39] IEC: Industrial communication networks – Wireless communication networks – Part 1: Wireless communication requirements and spectrum considerations, IEC TS 62657-1:2014

[40] NIST Special Publication 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations”, National Institute of Standards and Technology, U.S. Department of Commerce

[41] ISO/IEC 2382-14:1997 Information technology –Vocabulary—Part 14: Reliability, maintainability and availability, 1997

Published by
BZKI | Begleitforschung zur
zuverlässigen, drahtlosen
Kommunikation in der Industrie
Fachgruppe 1

Contact
ifak – Institut für Automation und
Kommunikation e.V. Magdeburg
Werner-Heisenberg-Str. 1
39106 Magdeburg

Sarah Willmann
E-Mail: sarah.willmann@ifak.eu

INDUSTRIAL® RADIO.DE