AS IEC 61131.6:2014
IEC 61131-6:2012

AS IEC 61131.6:2014

Australian STANDARD

Programmable controllers

Part 6: Functional safety

STANDARDS Australia

This Australian Standard® was prepared by Committee IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of the Council of Standards Australia on 28 May 2014.
This Standard was published on 27 June 2014.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Industry Group
- Australian Petroleum Production and Exploration Association
- Consult Australia
- Engineers Australia
- Institute of Chemical Engineers Australia
- Institute of Instrumentation, Control and Automation
- Process Control Society
- The University of Queensland
- Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR 102270.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Programmable controllers

Part 6: Functional safety

First published as AS IEC 61131.6:2014.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 1 74342 781 1

PREFACE

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

The objective of this Standard is to specify product-specific requirements of AS 61508.1—2011, AS 61508.2—2011 and AS 61508.3—2011 for functional safety programmable logic controllers (FS-PLC) and their associated peripherals. Some aspects do not have a direct correlation with the AS 61508 series structure and are addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc., in a single document.

This Standard should be read in conjunction with the other parts of the AS 61131 series.

This Standard is identical with and has been reproduced from IEC 61311-6, Ed.1.0 (2012) *Programmable controllers*, Part 6: *Functional Safety*.

As this Standard is reproduced from an International Standard, the following applies:

(a) Its number appears on the cover and title page, while the International Standard number appears only on the cover.

(b) In the source text, 'this part of IEC 61131' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian or Australian/New Zealand Standard*	
IEC		AS	
60947-5-1	Low-voltage switchgear and controlgear—Part 5-1: Control circuit devices and switching elements—Electromechanical control circuit devices	60947.5.1	Low-voltage switchgear and controlgear—Control circuit devices and switching elements—Electromechanical control circuit devices
61508	Functional safety of electrical/electronic/programmable electronic safety related systems	61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
61508-1	Part 1: General requirements	61508.1	Part 1: General requirements
61508-2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	61508.2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
61508-3	Part 3: Software requirements	61508.3	Part 3:Software requirements
61508-6	Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	61508.6	Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC		AS IEC	
61131	Programmable controllers	61131	Programmable controllers
61131-1	Part 1: General information	61131.1	Part 1:General information
61131-2	Part 2: Equipment requirements and tests	61131.2	Part 2:Equipment requirements and tests
61131-4	Part 4: User guidelines	61131.4	Part 4:User guidelines

IEC		AS/NZS	
61000	Electromagnetic compatibility (EMC)	61000	Electromagnetic compatibility (EMC)
61000-4-5	Part 4-5: Testing and measurement techniques—Surge immunity test	61000.4.5	Part 4.5: Testing and measurement techniques—Surge immunity test
61000-4-8	Part 4-8: Testing and measurement techniques—Power frequency magnetic field immunity test	61000.4.8	Part 4.8: Testing and measurement techniques—Power frequency magnetic field immunity test
IEC		AS/NZS IEC	
61000	Electromagnetic compatibility (EMC)	61000	Electromagnetic compatibility (EMC)
61000-4-2	Part 4-2: Testing and measurement techniques—Electrostatic discharge immunity test	61000.4.2	Part 4.2: Testing and measurement techniques—Electrostatic discharge immunity test
61000-4-3	Part 4-3: Testing and measurement techniques—Radiated, radio-frequency, electromagnetic field immunity test	61000.4.3	Part 4.3: Testing and measurement techniques—Radiated, radio-frequency, electromagnetic field immunity test
61000-4-4	Part 4-4: Testing and measurement techniques—Electrical fast transient/burst immunity test	61000.4.4	Part 4.4: Testing and measurement techniques—Electrical fast transient/burst immunity test

Only normative references that have been adopted as Australian or Australian/New Zealand Standard have been listed.

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a standard, whereas an informative annex is only for information and guidance.

CONTENTS

Page

Page

Page

INTRODUCTION

General

IEC 61131 series consists of the following parts under the general title *Programmable controllers*:

Part 1: General information
Part 2: Equipment requirements and tests
Part 3: Programming languages
Part 4: User guidelines
Part 5: Communications
Part 6: Functional safety
Part 7: Fuzzy control programming
Part 8: Guidelines for the application and implementation of programming languages

This Part of IEC 61131 series constitutes Part 6 of a series of standards on programmable controllers and the associated peripherals and should be read in conjunction with the other parts of the series.

As this document is the FS-PLC product standard, the provisions of this part should be considered to govern in the area of programmable controllers and their associated peripherals.

Compliance with Part 6 of IEC 61131 cannot be claimed unless the requirements of Clause 4 of this part are met.

Terms of general use are defined in Part 1 of IEC 61131. More specific terms are defined in each part.

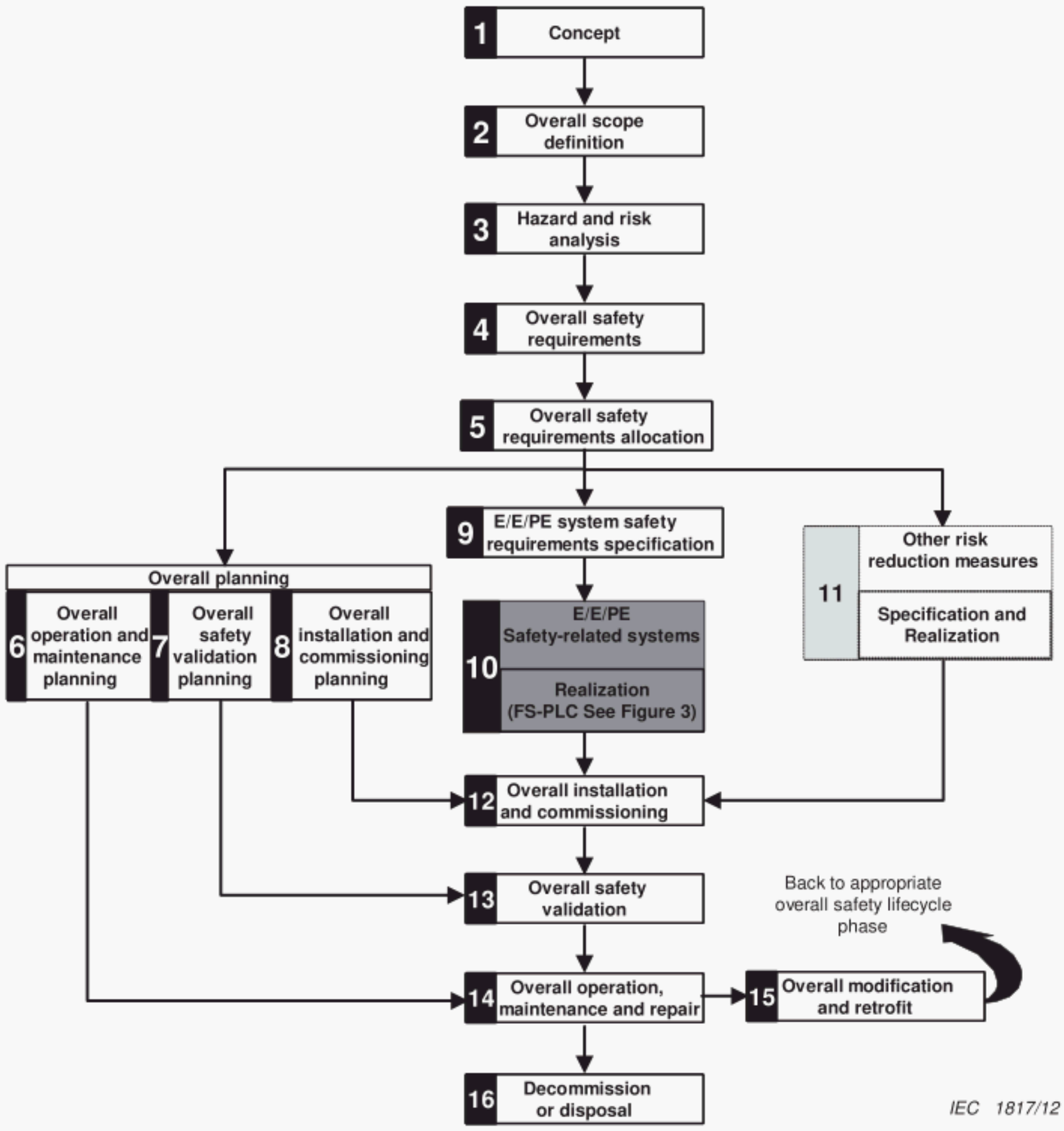
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

This document's intent is to follow the IEC 61508 series structure, in principle. But some aspects do not have a direct correlation and thus need to be addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc. in a single document.

Framework of this part

IEC 61508-1:2010, Figure 2 is included here, and is designated Figure 1. It has been adjusted to show how an FS-PLC fits into the overall E/E/PE safety-related system safety lifecycle. Though Figure 1 box 10 includes sensors, logic subsystem and final elements (e.g. actuators), from the viewpoint of IEC 61508-1, the FS-PLC is given emphasis here by including a reference to Figure 3.

As such, the Realization Phase, Figure 1, box 10, embodies only the logic subsystem, from this part's perspective.



NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phases represented by box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E? PE safety-related system and its elements and components.

Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases

The areas included in this part are FS-PLC safety lifecycle management, functional safety requirements allocation, and development planning; with the major emphasis on the Realization Phase (Box 10) of the overall safety lifecycle, shown in Figure 1. The assumption of this part is that the FS-PLC is utilized as a logic subsystem for the overall E/E/PE system.

The Figure 1, Realization (box 10), includes:

- the allocation of the FS-PLC safety aspects to FS-PLC hardware, software or firmware, or any combination,
- FS-PLC hardware architectures,
- verification and validation activities at the FS-PLC level,
- FS-PLC modification requirements,
- operation and maintenance information for the FS-PLC user,
- information to be provided by the FS-PLC manufacturer for the user.

AUSTRALIAN STANDARD

Programmable controllers

Part 6: Functional safety

1 Scope

This Part of the IEC 61131 series specifies requirements for programmable controllers (PLCs) and their associated peripherals, as defined in Part 1, which are intended to be used as the logic subsystem of an electrical/electronic/programmable electronic (E/E/PE) safety-related system. A programmable controller and its associated peripherals complying with the requirements of this part is considered suitable for use in an E/E/PE safety-related system and is identified as a functional safety programmable logic controller (FS-PLC). An FS-PLC is generally a hardware (HW) / software (SW) subsystem. An FS-PLC may also include software elements, for example predefined function blocks.

An E/E/PE safety-related system generally consists of sensors, actuators, software and a logic subsystem. This part is a product specific implementation of the requirements of the IEC 61508 series and conformity to this part fulfils all of the applicable requirements of the IEC 61508 series related to FS-PLCs. While the IEC 61508 series is a system standard, this part provides product specific requirements for the application of the principles of the IEC 61508 series to FS-PLC.

This Part of the IEC 61131 series addresses only the functional safety and safety integrity requirements of an FS-PLC when used as part of an E/E/PE safety-related system. The definition of the functional safety requirements of the overall E/E/PE safety-related system and the functional safety requirements of the ultimate application of the E/E/PE safety-related system are outside the scope of this part, but they are inputs for this part. For application specific information the reader is referred to standards such as the IEC 61511 series, IEC 62061, and the ISO 13849 series.

This part does not cover general safety requirements for an FS-PLC such as requirements related to electric shock and fire hazards specified in IEC 61131-2.

This part applies to an FS-PLC with a Safety Integrity Level (SIL) capability not greater than SIL 3.

The objective of this part is:

- to establish and describe the safety life-cycle elements of an FS-PLC, in harmony with the general safety life-cycle identified in IEC 61508-1, -2 and -3;
- to establish and describe the requirements for FS-PLC HW and SW that relate to the functional safety and safety integrity requirements of a E/E/PE safety-related system;
- to establish evaluation methods for a FS-PLC to this part for the following parameters/criteria:
  - a Safety Integrity Level (SIL) claim for which the FS-PLC is capable,
  - a Probability of Failure on Demand (PFD) value,
  - an average frequency of dangerous failure per hour value (PFH),
  - a value for the safe failure fraction (SFF),
  - a value for the hardware fault tolerance (HFT),
  - a diagnostic coverage (DC) value,
  - a verification that the specified FS-PLC manufacturer's safety lifecycle processes are in place,

  - the defined safe state,
  - the measures and techniques for the prevention and control of systematic faults, and
  - for each failure mode addressed in this part, the functional behaviour in the failed state;
- to establish the definitions and identify the principal characteristics relevant to the selection and application of FS-PLCs and their associated peripherals.

This part is primarily intended for FS-PLC manufacturers. It also includes the critical role of FS-PLC users through the user documentation requirements. Some user guidelines for FS-PLCs may be found in IEC 61131-4.

The requirements of ISO/IEC Guide 51 and IEC Guide 104, as they relate to this part, are incorporated herein.

2 Normative references

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

IEC 60947-5-1:2003, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC/TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2005, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2008, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:2009, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*

IEC 61131-1:2003, *Programmable controllers – Part 1: General information*

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-4:2004, *Programmable controllers – Part 4: User guidelines*

IEC 61326-3-1:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for*

equipment intended to perform safety-related functions (functional safety) – General industrial applications

IEC 61326-3-2:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-6:2010, *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 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC Guide 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

EN 50205:2002, *Relays with forcibly guided (mechanically linked) contacts*

3 Terms and definitions

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

3.1
application program
application software
part of the software of a programmable electronic system that specifies the functions that perform a task related to the EUC rather than the functioning of, and services provided by the programmable device itself

[SOURCE: IEC 61508-4:2010, 3.2.7]

3.2
application specific integrated circuit
ASIC
integrated circuit designed and manufactured for specific function, where its functionality is defined by the product developer

[SOURCE: IEC 61508-4:2010, 3.2.15]

3.3
architecture
specific configuration of hardware and software elements in a system

[SOURCE: IEC 61508-4:2010, 3.3.4]

3.4
availability
the probability that an item is able to perform its intended function, expressed as a decimal value between zero and one

EXAMPLE A = 0,9 means that a product is available 90 % of the time.

Note 1 to entry: For $\lambda T << 1$, $A = 1 - \lambda T$, See 3.23.

3.5
average frequency of a dangerous failure per hour
PFH
average frequency of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function over a given period of time

Note 1 to entry: The term “probability of dangerous failure per hour” is not used in this standard but the acronym PFH has been retained but when it is used it means “average frequency of dangerous failure [h]”.

Note 2 to entry: From a theoretical point of view, the PFH is the average of the unconditional failure intensity, also called failure frequency, and which is generally designated *w(t)*. It should not be confused with a failure rate (see Annex B of IEC 61508-6:2010).

Note 3 to entry: When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its unreliability $F(T)=1-R(t)$ (see failure rate above). When it is not the ultimate safety-related system its PFH should be calculated from its unavailability $U(t)$ (see PFD, 3.38). PFH approximations are given by $F(T)/T$ and 1/MTTF in the first case and 1/MTBF in the second case.

Note 4 to entry: When the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

[SOURCE: IEC 61508-4:2010, 3.6.19]

3.6
black channel
parts of a communication channel which are not designed or validated according to the IEC 61508 series

Note 1 to entry: See: 7.4.11.2 of IEC 61508-2:2010.

3.7
channel
element or group of elements that separately implement an element safety function

EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.

Note 1 to entry: The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

[SOURCE: IEC 61508-4:2010, 3.3.6]

3.8
common cause failure
CCF
failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure

[SOURCE: IEC 61508-4:2010, 3.6.10]

3.9
cyber security
protection of data in computer and information systems from loss or corruption due to intentional or unintentional activities by unauthorized or malicious individuals

Note 1 to entry: This term concerns the defence against such activities via network or other communication interfaces.

3.10
dangerous failure
FS-PLC
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,
b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.11
dangerous fault
fault that can lead to dangerous failure

Note 1 to entry: If a dangerous fault is detected, action is taken to avoid a dangerous failure.

3.12
defined safe state
the state of the FS-PLC, as defined by the FS-PLC manufacturer, when a dangerous failure occurs

Note 1 to entry: Typically, the defined safe state is the default state of each and every FS-PLC output. For digital outputs, this state is considered de-energized unless specifically defined otherwise. For analogue outputs, this state is zero volts or zero amps, unless specifically defined otherwise. For communications ports, this state is defined as no communications, unless specifically defined otherwise.

3.13
detected failure
termination of the ability of a functional unit to perform a required function detected by the diagnostic tests, proof tests, operator intervention or through normal operation

EXAMPLE Physical inspection and manual tests.

3.14
diagnostic coverage
DC

fraction of dangerous failures, detected by automatic on-line diagnostic tests, computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures

Note 1 to entry: The dangerous failure diagnostic coverage is computed using the following equation, where DC is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and λ_{Dtotal} is the total dangerous failure rate:

$$DC = \Sigma\lambda_{DD} / \Sigma\lambda_{Dtotal}$$

Note 2 to entry: This definition is applicable providing the individual components have constant failure rates.

[SOURCE: IEC 61508-4:2010, 3.8.6]

3.15
E/E/PE
electrical/electronic/programmable electronic

3.16
element
part of a subsystem comprising a single component or any group of components that performs one or more element safety functions

[SOURCE: IEC 62061:2005, 3.2.6, modified]

Note 1 to entry: An element may comprise hardware and/or software.

[SOURCE: IEC 61508-4:2010, 3.4.5, modified]

3.17
element safety function
that part of a safety function which is implemented by an element

[SOURCE: IEC 61508-4:2010, 3.5.3, modified]

3.18
embedded SW
embedded software
embedded firmware
FW
software controlling the operation of the FS-PLC or one of its subsystems

Note 1 to entry: The embedded software is supplied by the FS-PLC manufacturer installed in the FS-PLC. The user has no direct access to embedded software. The FS-PLC manufacturer develops or writes embedded software to control his FS-PLC. This may, for example, control the communication subsystem or the interpretation of the program developed by the user in the engineering tools.

Note 2 to entry: Another term for embedded software.

Note 3 to entry: Firmware can be either safety related or non-safety related.

3.19
engineering tools
software for developing the application program

EXAMPLE: The engineering tools software is supplied by the FS-PLC manufacturer to be installed on a personal computer workstation. Within this SW package the user develops or writes his application program to control his process. This application program is then downloaded into the FS-PLC, where it determines control of the user's FS-PLC, attached equipment and thus process.

Note 1 to entry: Application programs and software can be either safety related or non-safety related.

3.20
equipment under control
EUC
equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities

Note 1 to entry: The EUC control system is separate and distinct from the EUC.

[SOURCE: IEC 61508-4:2010, 3.2.1]

3.21
equipment under test
EUT
representative configuration(s), as defined by the manufacturer, used for type tests

3.22
failure
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required

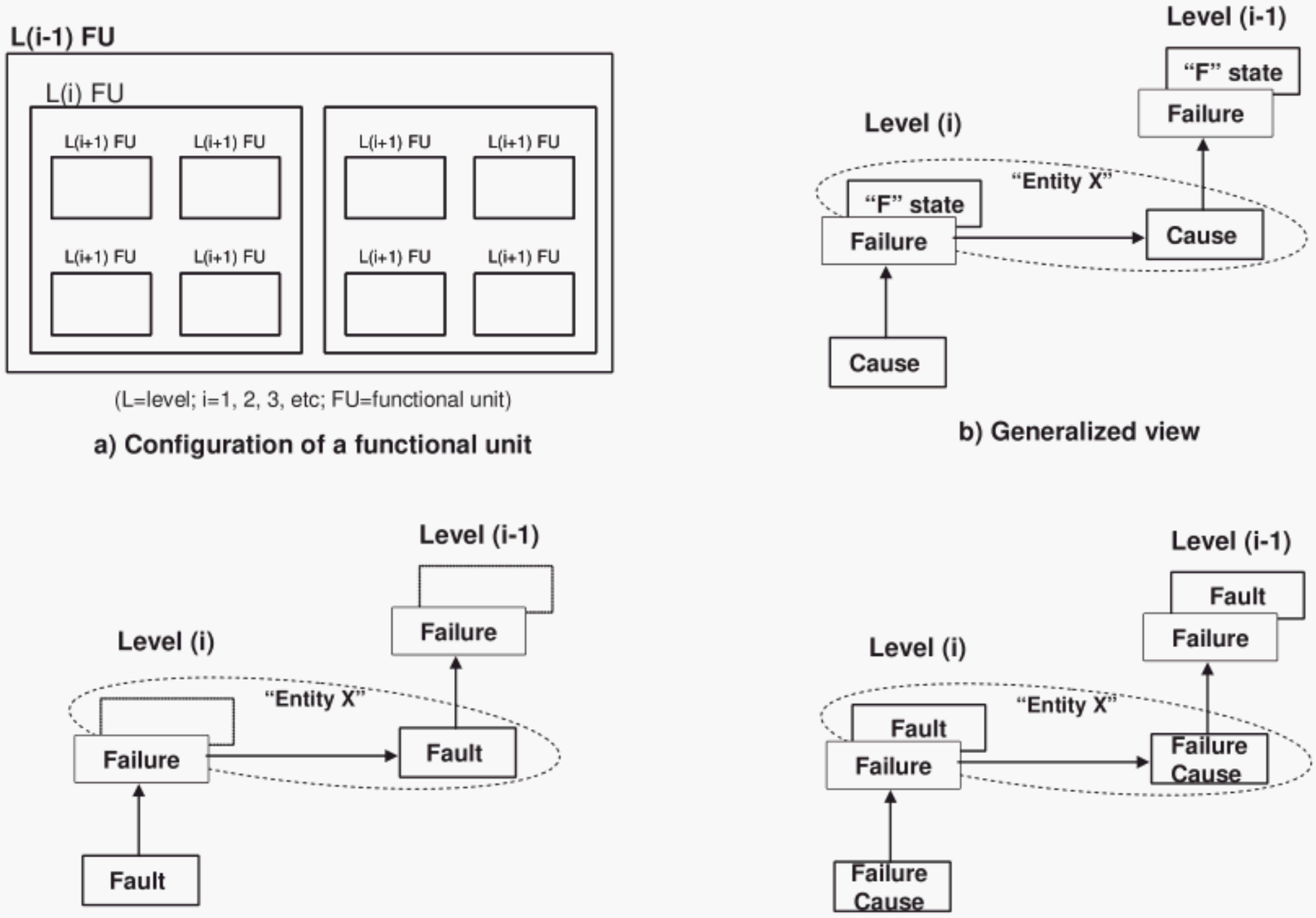
Note 1 to entry: This is based on IEC 60050-191:1990, 191-04-01 with changes to include systematic failures due to, for example, deficiencies in specification or software.

SEE: Figure 2 for the relationship between faults and failures.

Note 2 to entry: Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

Note 3 to entry: Failures are either random (in hardware) or systematic (in hardware or software), see 3.42 and 3.56.

[SOURCE: IEC 61508-4:2010, 3.6.4]



NOTE 1 As shown in a), a functional unit is able to be viewed as a hierarchical composition of multiple levels, each of which might in turn be called a functional unit. In level (i), a "cause" might manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, might cause a failure of this functional unit, as a result of which it falls into an "F" state where it is no longer able to perform a required function (see b)). This "F" state of the level (i) functional unit might in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, might cause a failure of this level (i-1) functional unit.

NOTE 2 In this cause and effect chain, the same thing ("Entity X") is able to be viewed as a state ("F" state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the failure of the level (i-1) functional unit. This "Entity X" combines the concept of "fault" in IEC 61508 series and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in c), and that of "fault" in IEC 60050-191, which emphasizes its state aspect as illustrated in d). The "F" state is called fault in IEC 60050-191, whereas it is not defined in IEC 61508 series and ISO/IEC 2382-14.

NOTE 3 In some cases, a failure or an error might be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

Figure 2 – Failure model

3.23
failure rate
reliability parameter ($\lambda(t)$) of an entity (single components or systems) such that $\lambda(t).dt$ is the probability of failure of this entity within [t, $t+dt$] provided that it has not failed during [0, t]

Note 1 to entry: Mathematically, λ(*t*) is the conditional probability of failure per unit of time over [*t, t+dt*]. It is in strong relationship with the reliability function (i.e. probability of no failure from 0 to *t*) by the general formula $R(t) = \exp(-\int_0^t \lambda(\tau)d\tau$. Reversely it is defined from the reliability function by $\lambda(t) = -\frac{dr(t)}{dt}\frac{1}{r(t)}$.

Note 2 to entry: Failure rates and their uncertainties can be estimated from field feedback by using conventional statistics. During the "useful life" (i.e. after burn-in and before wear-out), the failure rate of a simple items is more or less constant, $\lambda\ (t) \equiv \lambda$.

Note 3 to entry: The average of λ(*t*) over a given period [0, *T*], $\lambda_{avg}(T) = (\int_0^T \lambda(\tau)d\tau)/T$, is not a failure rate because it cannot be used for calculating *R*(*t*) as shown in Note 1 to entry. Anyway it may be interpreted as the average frequency of failure over this period (i.e. the PFH, see Annex B of IEC 61508-6:2010).

Note 4 to entry: The failure rate of a series of items is the sum of the failure rates of each items.

Note 5 to entry: The failure rate of redundant systems is generally non constant. Nevertheless when all failures are quickly revealed, independent and quickly repaired λ(*t*) converges quickly to an asymptotic value λ_{as} which is the equivalent failure rate of the systems. It should not be confused with the average failure rate described in Note 3 to entry which doesn't necessarily converge to an asymptotic value.

[SOURCE: IEC 61508-4:2010, 3.6.16]

3.24
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

[SOURCE: ISO/IEC 2382-14:1997, 14.01.10]

Note 1 to entry: IEC 60050-191:1990, 191-05-01 defines “fault” as a state characterised by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources. See Figure 2 for an illustration of these two points of view.

[SOURCE:IEC 61508-4:2010, 3.6.1]

3.25
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

[SOURCE: ISO/IEC 2382-14:1997, 14.04.06]

Note 1 to entry: The definition in IEC 60050-191:1990, 191-15-05 refers only to sub-item faults. See the Note 1 to entry in 3.24.

[SOURCE: IEC 61508-4:2010, 3.6.3]

Note 2 to entry: Faults and errors to be considered include those involving interfaces to the FS-PLC.

3.26
FS-PLC functional safety requirements specification
specification containing the safety function requirements and associated safety integrity levels for the FS-PLC

3.27
functional safety
part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12]

Note 1 to entry: Functional safety is, in essence, the ability of a safety-related system to achieve or maintain a safe state.

3.28
HW
hardware
FS-PLC electrical, mechanical or other physical devices which are connected together to perform functions

3.29
high complexity safety-related subsystem
part of a E/E/PE safety-related system for which:

the failure mode of at least one component is not well defined, or

the behaviour of the subsystem under fault conditions cannot be completely determined, or

there is insufficient field failure data to show that the claimed failure rates are met

EXAMPLE A FS-PLC. This is derived from type B subsystem as described in IEC 61508-2:2010, 7.4.4.1.3.

Note 1 to entry: Refer to Type A (9.4.3.2.2) and Type B (9.4.3.2.3) systems.

3.30
logic subsystem
a logic subsystem is defined as that portion of a E/E/PE safety-related system that performs the function logic but excludes sensors and final elements

EXAMPLE An FS-PLC is a logic subsystem.

3.31
mean repair time
MRT
expected overall repair time

Note 1 to entry: MRT encompasses the times (b), (c) and (d) of the times for MTTR (see 3.34).

[SOURCE: IEC 61508-4:2010, 3.6.22]

3.32
mean time between failures
MTBF
a statistically based parameter (usually expressed in hours) that allows comparisons to be made between the reliability of different products

Note 1 to entry: Mathematically, it is the reciprocal of a repairable product's failure rate.

Note 2 to entry: MTBF is an arithmetic mean determined from a large number of units over a long period of time.

Note 3 to entry: For a complex product like a PLC, the average failure rate approximates a constant failure rate with an exponential Reliability function: $R(t) = e^{-\lambda t}$

Note 4 to entry: MTBF = MTTF + MTTR.

SEE: NOTE 2 to entry of 3.33.

3.33
mean time to failure
MTTF
a statistically based parameter (usually expressed in hours) that allows comparisons between the reliability of different non-repairable products

Note 1 to entry: For a non-repairable product with a constant failure rate, MTTF is the reciprocal of the product's failure rate.

Note 2 to entry: MTTF is an arithmetic mean determined from a large number of units over a long period of time.

Note 3 to entry: Although the two terms MTBF and MTTF are sometimes used interchangeably, they are properly used to refer to repairable and non-repairable products respectively. MTBF should be used only for products that are normally repaired and returned to service.

3.34
mean time to restoration
MTTR

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

the time to detect the failure (a); and,

the time spent before starting the repair (b); and,

the effective time to repair (c); and,

the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

[SOURCE: IEC 61508-4:2010, 3.6.21]

3.35
mode of operation
way in which a safety function operates, which may be either low demand, high demand or continuous mode

Note 1 to entry: The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2:2010).

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.1
low demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.2
high demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.3
continuous mode
where the safety function retains the EUC in a safe state as part of normal operation

[SOURCE: IEC 61508-4:2010, 3.5.14]

3.36
MooN
M out of N
architecture made up of “N” independent channels, which are so connected, that at least “M” channels are required to perform the safety function

Note 3 to entry: Although the two terms MTBF and MTTF are sometimes used interchangeably, they are properly used to refer to repairable and non-repairable products respectively. MTBF should be used only for products that are normally repaired and returned to service.

3.34
mean time to restoration
MTTR

expected time to achieve restoration

Note 1 to entry: MTTR encompasses:

the time to detect the failure (a); and,

the time spent before starting the repair (b); and,

the effective time to repair (c); and,

the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

[SOURCE: IEC 61508-4:2010, 3.6.21]

3.35
mode of operation
way in which a safety function operates, which may be either low demand, high demand or continuous mode

Note 1 to entry: The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508-2:2010).

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.1
low demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.2
high demand mode
where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16]

3.35.3
continuous mode
where the safety function retains the EUC in a safe state as part of normal operation

[SOURCE: IEC 61508-4:2010, 3.5.14]

3.36
MooN
M out of N
architecture made up of “N” independent channels, which are so connected, that at least “M” channels are required to perform the safety function

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC

3.42
random hardware failure
failure, occurring at a random time, that results from one or more of the possible degradation mechanisms in the hardware

Note 1 to entry: There are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising many components occur at predictable rates but at unpredictable (i.e. random) times.

Note 2 to entry: A major distinguishing feature between random hardware failures and systematic failures (see 3.56), is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.

[SOURCE: IEC 61508-4:2010, 3.6.5]

3.43
reliability
R
probability that a specific product will operate for a specific duration/time (t) without a failure

Note 1 to entry: For a complex product like a programmable controller, the average failure rate approximates a constant failure rate with an exponential reliability function: $R(t) = e^{-\lambda t} = e^{-(t/MTBF)}$.

Note 2 to entry: If the time (t) in the last equation is the MTBF, the equation yields a reliability of 0,368 meaning that only 36,8 % of a specific product will operate without a failure for their MTBF.

3.44
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:1999, definition 3.2]

Note 1 to entry: For more discussion on this concept, see Annex A of IEC 61508-5:2010.

[SOURCE: IEC 61508-4:2010, 3.1.6]

3.45
safe failure
FS-PLC