IEC TS 62998-1

Edition 1.0 2019-05

TECHNICAL SPECIFICATION

Safety of machinery – Safety-related sensors used for the protection of persons

IEC TS 62998-1:2019-05(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC TS 62998-1

Edition 1.0 2019-05

TECHNICAL SPECIFICATION

colour
inside

Safety of machinery – Safety-related sensors used for the protection of persons

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 21.020

ISBN 978-2-8322-6819-3

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD ... 6
INTRODUCTION ... 8
1 Scope ... 9
2 Normative references ... 10
3 Terms and definitions ... 10
3.1 Characteristics and performance criteria ... 11
3.2 Dependability ... 12
3.3 Procedures and architectural deliberations ... 14
3.4 Terms related to system ... 16
3.5 Fusion ... 18
3.6 Safety related information ... 18
3.7 Test ... 20
3.8 User groups ... 22
3.9 Verification and validation ... 22
4 Lifecycle and interconnection to safety-related electrical control systems (SCS) ... 24
4.1 General ... 24
4.2 Hazard and risk analysis ... 26
4.2.1 General ... 26
4.2.2 Hazard caused by SRS/SRSS ... 27
4.2.3 Required SRS/SRSS performance class ... 28
4.3 Correspondence SRS/SRSS performance class ... 28
5 Design and development phase ... 29
5.1 General ... 29
5.2 SRS/SRSS functions ... 29
5.3 Design analysis ... 30
5.4 Simulation ... 30
5.5 Sensing zone(s) ... 31
5.6 Safety related zone ... 31
5.7 Automation related zone ... 31
5.8 Detection capability and dependability ... 31
5.8.1 General ... 31
5.8.2 Object classes and physical properties ... 32
5.8.3 Environmental influences ... 33
5.9 User interface ... 37
5.9.1 General ... 37
5.9.2 Mounting ... 37
5.9.3 Safety related information ... 37
6 Integration and installation phase ... 40
6.1 General ... 40
6.2 Fusion of SRS into an SRSS ... 40
6.2.1 General ... 40
6.2.2 Limits of use after fusion ... 41
6.2.3 Detection capability after fusion ... 41
6.2.4 Sensing zone(s) after fusion ... 42
6.2.5 Dependability under environmental condition after fusion ... 42
6.2.6 Safety related information after fusion ... 42

6.2.7 SRSS performance class after fusion 43
6.2.8 Response time after fusion 44
6.2.9 Verification and validation after fusion 44
6.3 Calibration at user side 44
6.3.1 General 44
6.3.2 Calibration procedure and equipment 45
6.3.3 Verification and validation of calibration 45
7 Operation, maintenance and modification phases 45
8 Verification and validation 46
8.1 General 46
8.2 Verification of an SRS/SRSS 46
8.3 Validation of an SRS/SRSS 47
8.4 Analysis 48
8.5 Test 49
8.5.1 General 49
8.5.2 Test classification 49
8.5.3 Test method and test setup 50
8.5.4 Test piece 51
8.5.5 Test plan and test results 51
9 Information for use 52
Annex A (informative) Examination of systematic capabilities 54
Annex B (informative) User groups 55
B.1 User groups of SRS/SRSS and groups addressed by this document 55
B.2 User groups addressed by fusion 55
Annex C (informative) Functional decomposition and/or integration 58
Annex D (normative) Generation and application of simulation models 59
D.1 General 59
D.2 Recommendations for use 59
D.3 Simulation objectives and measures to achieve them 59
D.4 Verification 62
Annex E (informative) Child properties and behaviour 64
E.1 General 64
E.2 Sizes of parts of body 64
Annex F (informative) Environmental influences 68
F.1 General 68
F.2 Example 1 for application of environmental influences 68
F.3 Example 2 for application of environmental influences 70
Annex G (informative) Faults, failures and influences resulting in a loss of SRS/SRSS safety related function 71
G.1 General 71
G.2 Failure to danger 74
G.3 Normal operation 75
G.4 Signal to initiate the fault reaction function and confidence information as part of safety related information 75
Annex H (informative) Test aspects 77
H.1 General 77
H.2 Mechanical influence test 77
Annex I (informative) Examples of functions, safety related information and fusion 81

I.1 Example of functions 81
I.2 Example of safety related information 82
I.3 Example of fusion 83
Bibliography 87

Figure 1 – Measurement accuracy and measurement uncertainty 12
Figure 2 – Example 1 of SRS architecture 24
Figure 3 – Example 2 of SRS architecture 25
Figure 4 –Example of SRSS architecture 25
Figure 5 – Interconnection of an SRS/SRSS into hazard and risk analysis 27
Figure 6 – Safety related information of an SRS/SRSS 38
Figure A.1 – Example for examination of systematic capabilities using safety related sensor standards 54
Figure C.1 – Interconnection of functions and objects 58
Figure C.2 – Example of functions performed in an SRSS 58
Figure D.1 – Verification process 62
Figure E.1 – Body height children 65
Figure E.2 – Chest depth children 66
Figure E.3 – Head width children 66
Figure E.4 – Head length children 67
Figure G.1 – Combination of faults, failures or errors resulting in additional risk throughloss of safety function or bypassing 72
Figure G.2 – Analysis of systematic capabilities during design and development to prevent systematic faults resulting in failure to danger 73
Figure G.3 – Mode of action for systematic fault resulting in fault reaction function 76
Figure G.4 – Mode of action for errors resulting in appropriate confidence information 76
Figure I.1 – Example of SRS applied on driveway intersection 81
Figure I.2 – Example of SRS/SRSS providing decision and confidence information 82
Figure I.3 – Example of SRS/SRSS providing measurement and confidence information 83
Figure I.4 – First example of fusion of 2 SRS into an SRSS with combined sensing zones 84
Figure I.5 – Fusion of SRS safety related information 84
Figure I.6 – Approach of verification and validation based on SRS Information for use and SRSS Safety Requirement specification 85
Figure I.7 – Second example of fusion of 2 SRS into an SRSS with combined sensing zones 86

Table 1 – Correspondence between level of safety performance and minimum required SRS/SRSS performance class 29
Table 2 – Functions of an SRS/SRSS as applicable 30
Table 4 – Limits for failure to danger condition (loss of the detection capability) due to environmental interference for high demand mode 35
Table 5 – Minimum required coverage probability/decision probability at high demand rate 39
Table 6 – Maximum applicable SRSS performance class after fusion using two SRS 44

Table 7 – Means to be used for evaluation of verification measures and verification results 47

Table 8 – Overview of information for use to be provided 52

Table B.1 – Roles and task of addressed user groups 55

Table B.2 – Addressed user groups for different integration types using sensing unit, SRS/ SRSS as element or SRS as subsystem 56

Table D.1 – Simulation objectives and measures for SRS/SRSS of low complexity 60

Table D.2 – Simulation objectives and measures for SRS/SRSS of high complexity 61

Table E.1– Body height children 64

Table E.2 – Chest depth children 65

Table E.3 – Head width children 66

Table E.4 – Head length children 67

Table F.1 – Example 1 of environmental influence and classes according to IEC 60721-3-5 69

Table F.2 – Example 2 of environmental influence and classes according to IEC 60721-3-3 70

Table G.1 – Demand rates used for the calculation of Table G.2 values 74

Table G.2 – Limits for failure to danger condition (loss of the detection capability) due to environmental influence for high demand mode 74

Table H.1 – Example of test plan and test result for mechanical influence test 78

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SAFETY OF MACHINERY –

Safety-related sensors used for the protection of persons

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a Technical Specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical Specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 62998-1, which is a Technical Specification, has been prepared by IEC technical committee TC 44: Safety of machinery – Electrotechnical aspects.

The text of this Technical Specification is based on the following documents:

Draft TS	Report on voting
44/826/DTS	44/839A/RVDTS

Full information on the voting for the approval of this Technical Specification can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62998 series, published under the general title *Safety of machinery*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Safety related sensors are applied to machinery presenting a risk of personal injury. They provide protection by causing the machine to revert to a safe condition before a person can be placed in a hazardous situation.

IEC 61496 (all parts) provides design and performance requirements of electro-sensitive protective equipment (ESPE). It gives a clear but limited guideline for

- specific sensor technologies (like optical sensors) or sensing functions (like capability to detect a specified object);
- typical conditions representing indoor use in industrial environment;
- detection of objects representing parts of body of adults using the properties geometry and reflectivity;
- design, functional requirements and tests in accordance with ESPE specific safety performance classification in types (2,3 and 4).

Autonomous systems like automated guided vehicles (AGV), service robotics or human machine interaction in industries show an increasing demand, for example in

- new sensor technologies (e.g. radar, ultrasonic sensors),
- new kind of sensor functions (e.g. classification of objects, position of an object), and
- combination of different sensor technologies in a sensor system.

Sensor manufacturers or integrators use in such cases generic functional safety standards as guideline for the safety related product design. Generic functional safety standards like IEC 61508 (all parts) or sector specific machinery standards like IEC 62061 or ISO 13849 (all parts) are general and product design can be carried out without inappropriate limitations. Applying these standards would require a dedicated analysis of systematic capabilities of a sensor or sensor system (e.g. dependability of the sensing function under tolerance conditions and environmental influences). There is not enough guidance given in these standards to prevent design failures or insufficient capability to detect the specified object in certain environmental conditions. This can result in an intolerable risk for persons.

This document fills the gap for the examination of systematic capabilities between design specific sensor standards and generic functional safety standards of electrical, electronic or programmable electronic control systems.

NOTE 1 Examples for the examination of systematic capabilities by using different safety related sensor standards are given in Annex A.

This document is addressed to safety related sensor manufacturers and integrators of safety related sensors into a safety related sensor system.

NOTE 2 Examples for addressed user groups are given in Annex B.

SAFETY OF MACHINERY –

Safety-related sensors used for the protection of persons

1 Scope

This Technical Specification gives requirements for the development and integration of safety related sensors (SRS) and safety related sensor systems (SRSS) used for protection of persons with special attention to systematic capabilities.

This generic standard only applies if

- protection of persons is to be performed by using sensors, and
- standards for functional safety of electrical control systems address sensor(s) as subsystem or subsystem element, and
- product specific sensor standards (e.g. IEC 61496 (all parts), IEC 60947-5-2) do not contain all necessary provisions, or product specific sensor standards are not developed.

The approach of examination of systematic capabilities by using different safety related sensor standards is described in Annex A.

The requirements and methods within this document are limited to the purpose of protection of persons

- by detection of potentially hazardous objects,
- by detection of a body, parts of a body and objects associated to parts of a body entering a hazardous area, or
- by classification respective discrimination of these against other objects.

NOTE 1 Application of SRS/SRSS in public can require detecting not only of persons, but also their associated equipment, for example wheelchairs, walking sticks or infusion stands.

Performance classes of sensors and sensor systems are defined in accordance with existing functional safety standards (e.g. IEC 62061, IEC 61508 (all parts), and ISO 13849 (all parts)).

NOTE 2 There will be no definitions of or interconnections to the types as defined in IEC 61496-1 within this document to simplify and prevent misuse. Simplification for end users is achieved by correlation to existing PL, SIL or SIL$_{cl}$.

Special attention is given to the sensing function and dependability of the detection capability. Environmental influences and tests for indoor and outdoor use are defined which influence the sensing function and dependability of the detection capability.

NOTE 3 Environmental influences, their classification and test procedures are primarily specified in accordance with generic environmental standards. More specific requirements and tests are only described in absence of respective standards.

This document can be relevant to applications other than those for the protection of persons in industries, for example, for the protection of persons in public like agriculture or metro stations.

This document does not consider and address proven in use (e.g. processes or elements) as done in IEC 61508-2.

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 60068 (all parts), *Environmental testing*

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 60721 (all parts), *Classification of environmental conditions*

IEC 60825-1, *Safety of laser products – Part 1: Equipment classification and requirements*

IEC 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61496-1:2012, *Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests*

IEC 62061:2005, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*
IEC 62061:2005/AMD1:2012
IEC 62061:2005/AMD2:2015

IEC 62471, *Photobiological safety of lamps and lamp systems*

ISO 7250 (all parts), *Basic human body measurements for technological design*

ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

ISO 25119 (all parts), *Tractors and machinery for agriculture and forestry – Safety-related parts of control systems*

ISO 26262 (all parts), *Road vehicles – Functional safety*

CEN/CENELEC Guide 14*, Child safety – Guidance for its inclusion in standards*

3 Terms and definitions

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

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

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

3.1 Characteristics and performance criteria

3.1.1
automation related zone
part of the sensing zone within which specified objects(s) are detected in order to perform an automation related function

3.1.2
safety-related zone
part of the sensing zone within which specified safety related object(s) will be detected

3.1.3
sensing zone
zone defined by length, area or volume within which objects are detected and an SRS or SRSS function is performed

3.1.4
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant safety manual for the element

Note 1 to entry: Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

Note 2 to entry: What a relevant systematic failure mechanism is, will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.

Note 3 to entry: A systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

[SOURCE: IEC 61508-4:2010, 3.5.9]

3.1.5
detection
determination of the presence and/or value of a physical property

Note 1 to entry: As example classification can be a step of detection containing other steps like reception of physical signal and filtering.

3.1.6
detection capability
ability to perform the detection within the limits of use as specified by the manufacturer

3.1.7
loss of detection capability
event of SRS/SRSS when detection is not achieved within the limits of use as specified by the manufacturer

Note 1 to entry: A loss of detection could result from a degradation of detection capability. A degradation could be of interest for analysis of reduced integrity of detection resulting in a dangerous state.

3.1.8
physical property
individual measurable property of an object being observed

3.1.9
measurement accuracy
accuracy of measurement
accuracy
closeness of agreement between a measured quantity value and a true quantity value of a measurand

SEE: Figure 1.

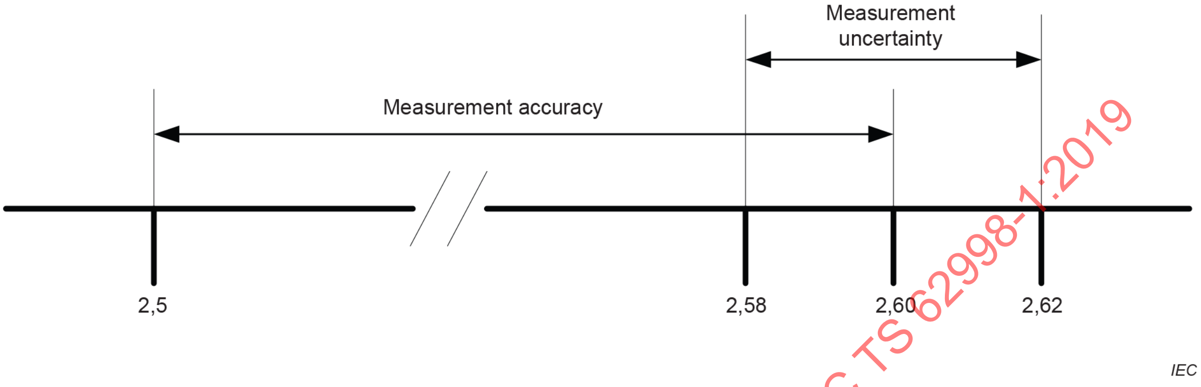


Figure 1 – Measurement accuracy and measurement uncertainty

[SOURCE: ISO/IEC Guide 99:2007, 2.13, modified – The notes to entry have been removed, and the figure has been added.]

3.1.10
measurement uncertainty
non-negative parameter characterizing the dispersion of the quantity values being attributed to a measurand, based on the information used

[SOURCE: ISO/IEC Guide 99:2007, 2.26, modified – The two other terms "uncertainty of measurement" and "uncertainty" has been removed as well as the notes to entry.]

3.2 Dependability

3.2.1
availability
ability to be in a state to perform as required

Note 1 to entry: Availability depends upon the combined characteristics of the reliability (192-01-24), recoverability (192-01-25), and maintainability (192-01-27) of the item, and the maintenance support performance (192-01-29).

Note 2 to entry: Availability may be quantified using measures defined in Section 192-08, *Availability related measures*.

[SOURCE: IEC 60050-192:2015, 192-01-23]

3.2.2
dependability
ability to perform as and when required

Note 1 to entry: Dependability includes availability (192-01-23), reliability (192-01-24), recoverability (192-01-25), maintainability (192-01-27), and maintenance support performance (192-01-29), and, in some cases, other characteristics such as durability (192-01-21), safety and security.

Note 2 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: IEC 60050-192:2015, 192-01-22, modified – The specific use "of an item" given after the term has been removed.]

3.2.3
reliability

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

Note 1 to entry: The time interval duration can be expressed in units appropriate to the item concerned, for example calendar time, operating cycles, distance run, etc., and the units should always be clearly stated.

Note 2 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 3 to entry: Reliability can be quantified using measures defined in Section 192-05, *Reliability related concepts: measures*.

[SOURCE: IEC 60050-192:2015, 192-01-24, modified – The specific use "of an item" given after the term has been removed.]

3.2.4
error

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

[SOURCE: IEC 60050-192:2015, 192-03-02, modified – The notes to entry have been removed.]

3.2.5
failure

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

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

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

Note 3 to entry: This concept, as defined, does not apply to items consisting of software only.

Note 4 to entry: In practice, the terms "fault" and "failure" are often used synonymously.

3.2.6
failure to danger

failure which results in the inability to perform the safety related function within the stated response time

3.2.7
fault

inability to perform as required, due to an internal state

Note 1 to entry: A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance. See latent fault (192-04-08).

Note 2 to entry: Qualifiers, such as specification, design, manufacture, maintenance or misuse, may be used to indicate the cause of a fault.

Note 3 to entry: The type of fault may be associated with the type of associated failure, for example wear-out fault and wear-out failure.

Note 4 to entry: The adjective "faulty" designates an item having one or more faults.

[SOURCE: IEC 60050-192:2015, 192-04-01, modified – The specific use "of an item" given after the term has been removed.]

3.3 Procedures and architectural deliberations

3.3.1

risk analysis

systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO/IEC Guide 51:2014, 3.10]

3.3.2

risk reduction measure

protective measure

action or means to eliminate hazards or reduce risks

EXAMPLE Inherently safe design; protective devices; personal protective equipment; information for use and installation; organization of work; training; application of equipment; supervision.

[SOURCE: ISO/IEC Guide 51:2014, 3.13]

3.3.3

tolerable risk

level of risk that is accepted in a given context based on the current values of society

[SOURCE: ISO/IEC Guide 51:2014, 3.15, modified – The note to entry has been removed.]

3.3.4

design and development

activities that take an idea or requirement and transform these into a product

Note 1 to entry: The process of design and development usually follows a series of defined steps starting with an initial idea, transforming that into a formal specification, and resulting in the creation of a working prototype and whatever documentation is required to support production of the goods or provision of the service.

[SOURCE: IEC 62430:2009, 3.1]

3.3.5

simulation

modelling of an SRS/SRSS or of subparts via calculation or via a software behavioural model used for a systematic and/or stochastic analysis of functional performance and the correct dimensioning and interaction of its subsystems

3.3.6

calibration

set of operations which establishes, by reference to standards, the relationship which exists, under specified conditions, between an indication and a result of a measurement

Note 1 to entry: This term is based on the "uncertainty" approach.

Note 2 to entry: The relationship between the indications and the results of measurement can be expressed, in principle, by a calibration diagram.

Note 3 to entry: Standards used as reference could be scale of length objects located in the sensing zone continuously or temporarily.

Note 4 to entry: Within this document, only calibration at the user side is specifically addressed. Calibration used during production of an SRS/SRSS is a measure which can be used to achieve the stated detection capability at manufacturer side, is part of analysis during design and development and not specifically addressed.

[SOURCE: IEC 60050-311:2001, 311-01-09, modified – Notes 3 and 4 to entry have been added.]

3.3.7
calibration procedure
documented, verified, and validated procedure that specifically describes a set of operations used in the performance of particular measurements according to a given method

Note 1 to entry: Calibration procedure used in the context of this document includes both calibration and adjustment.

[SOURCE: IAS Calibration and testing laboratory accreditation programs definitions, 2018, modified – The note to entry has been added.]

3.3.8
machinery
machine assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term "machinery" also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

Note 2 to entry: Annex A of ISO 12100:2010 provides a general schematic representation of a machine.

[SOURCE: ISO 12100:2010, 3.1, modified – The second term "machine" has been removed, but added to the definition before "assembly".]

3.3.9
safety-related system
designated system that both

– implements the required safety functions necessary to achieve or maintain a safe state for the EUC (equipment under control); and
– is intended to achieve, on its own or with other E/E/PE safety related systems and other risk reduction measures, the necessary safety integrity for the required safety functions

[SOURCE: IEC 61508-4:2010, 3.4.1, modified – The notes to entry have been removed.]

3.3.10
safety-related electrical control system
SCS
part of the control system of a machine which implements a safety function

Note 1 to entry: A SCS is the combination of one or more subsystems necessary to implement the respective safety sub-function(s).

Note 2 to entry: SCS is similar to SRECS of IEC 62061:2005.

Note 3 to entry: A machine has as many SCS as it has safety functions. One SCS is dedicated to one safety function of the machine.

Note 4 to entry: SCS has a different meaning to safety-related system from IEC 61508-4:2010, 3.4.1.

3.3.11
safety-related sensor
SRS
one or more sensing units combined to perform the safety related function

Note 1 to entry: An SRS can be regarded as a subsystem in a SCS or as a subsystem element in a SCS if the SRS is used as part of an SRSS.

Note 2 to entry: A sensing unit might contain one or more sensing elements.

3.3.12
safety-related sensor system
SRSS
combination of two or more safety-related sensors performing the safety related function

3.3.13
electro-sensitive protective equipment
ESPE
assembly of devices and/or components working together for protective tripping or presence-sensing purposes and comprising as a minimum

- a sensing device;
- controlling/monitoring devices;
- output signal switching devices and/or a safety related data interface

Note 1 to entry: An ESPE is a protective device used as risk reduction measure.

[SOURCE: IEC 61496-1:2012, 3.5, modified – The notes to entry have been replaced by a new Note 1 to entry.]

3.4 Terms related to system

3.4.1
subsystem
entity of the top-level architectural design of the SCS where a dangerous failure of any subsystem will result in a dangerous failure of a safety related control function

Note 1 to entry: A complete subsystem can be made up from a number of identifiable and separate subsystem elements, which when put together implement the function blocks allocated to the subsystem.

Note 2 to entry: This differs from common language where "subsystem" may mean any subdivided part of an entity, the term "subsystem" is used in IEC 62061 within a strongly defined hierarchy of terminology: "subsystem" is the first level subdivision of a system. The parts resulting from further subdivision of a subsystem are called "subsystem elements".

[SOURCE: IEC 62061:2005, IEC 62061:2005/AMD1:2012 and IEC 62061:2005/AMD2:2015, 3.2.5, modified – The abbreviated term "SRECS" has been replaced with "SCS" in the definition.]

3.4.2
subsystem element
part of a subsystem comprising a single component or any group of components that performs one or more element functions

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

[SOURCE: IEC 62061:2005, 3.2.6, modified – The words "that performs one or more element functions" have been added to the definition, and Note 1 to entry has been added.]

3.4.3
complexity
property of a SRS/SRSS or a safety function that is characterized by multiple subsystem elements or sub-functions interacting in a non-trivial way

Note 1 to entry The degree of complexity of an SRS/SRSS may depend on the role or perspective within the supply chain. While an SRS under development can be judged highly complex by the manufacturer due to its many interacting subsystem elements and the number of external influences that have to be taken into account, an integrator who employs it within the limits of intended use might model it as a black box system with few defined outputs and judge it to be of low complexity.

Note 2 to entry: The detailed behavior of a complex system or complex function is not accessible by simple calculation

3.4.4
demand rate

number of events that occur in a defined time which cause the SRS/SRSS to perform its safety related function

Note 1 to entry: Low demand mode is a mode of operation in which the safety related function of an SRS/SRSS is only performed on demand and where the demand rate is no greater than one per year.

Note 2 to entry: High demand mode is a mode of operation in which the safety related function of an SRS/SRSS is only performed on demand and where the demand rate is greater than one per year. As an orientation, high demand rates are given in Table G.1 (stated values are in accordance with ISO 13849 (all parts)).

Note 3 to entry: Continuous mode is a mode of operation in which the safety related function of an SRS/SRSS is performed perpetually (continuously). Finally, the limiting factor for the applicable demand rate in continuous mode is the response time of the SRS/SRSS.

Note 4 to entry: The demand rate for the safety related functions of the SRS/SRSS can be different than the demand rate for the safety function performed in a SCS.

3.4.5
safe state

state of the EUC (equipment under control) when safety is achieved

EXAMPLE 1 The safe state might be initiated by the decision information.

EXAMPLE 2 The safe state might be initiated by the confidence information.

Note 1 to entry: The safe state might be related to different output signals depending on the intended use and performed SRS/SRSS function.

[SOURCE: IEC 61508-4:2010, 3.1.13, modified – The examples has been added, and the note to entry has been replaced by a new note.]

3.4.6
normal operating condition

operating condition that represents as closely as possible the range of normal use that can reasonably be expected

[SOURCE: IEC 62368-1:2018, 3.3.7.4, modified – The words "mode of operation" have been replaced by "operating condition" in the definition, and the notes to entry have been removed.]

3.4.7
normal operation

state of a SRS/SRSS where it operates as specified and where no faults are detected

3.4.8
intended use

use in accordance with information provided with a product or system, or, in the absence of such information, by generally understood patterns of usage

[SOURCE: ISO/IEC Guide 51:2014, 3.6]

3.4.9
limit of use

definition of limits on achieved detection capability, sensing zone, environmental, mounting, safety related information at the output unit and SRS/SRSS performance class provided by the manufacturer of an SRS/SRSS or integrator of SRS into an SRSS

Note 1 to entry: The limits of use are essential to validate if the SRS/SRSS is appropriate for the application respective the intended use.

3.5 Fusion

3.5.1
alignment
processing of SRS measurements to achieve a common time base and a common spatial reference

3.5.2
diversity
different means of performing a required function

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

[SOURCE: IEC 61508-4:2010, 3.3.7]

3.5.3
fusion
act or process of combining or associating data or information regarding one or more entities considered in an explicit or implicit knowledge framework to improve one’s capability (or provide a new capability) for detection, identification, or characterization of that entity

3.5.4
redundancy
provision of more than one means for performing a function

Note 1 to entry: The additional means of performing the function can be intentionally different (diverse) to reduce the potential for common mode failures (192-03-19).

[SOURCE: IEC 60050-192:2015, 192-10-02, modified – The specific use "of a system" given after the term has been removed]

3.6 Safety related information

3.6.1
analog signal
signal which directly represents the respective variable quantity

Note 1 to entry: An analog signal may be a continuous-value or a discrete-value signal as well as a continuous-time or a discrete-time signal. Examples may be the pressure in a pneumatic final controlling element with continuous-value and continuous-time information parameter (value of the pressure) as well as a position-modulated pulse signal as an output signal of a computer based controller.

Note 2 to entry: This entry was numbered 351-21-53 in IEC 60050-351:2006.

[SOURCE: IEC 60050-351:2013, 351-41-24, modified – The words "each information parameter of" have been removed from the definition.]

3.6.2
coverage interval
interval containing the set of true quantity values of a SRS/SRSS measurement information with a stated probability, based on the information available

Note 1 to entry: A coverage interval does not need to be centered on the chosen measured quantity value (see ISO/IEC Guide 98-3:2008/Supplement 1)

[SOURCE: ISO/IEC Guide 99:2007, 2.36, modified – The word "measurand" has been replaced by "SRS/SRSS measurement information", and Note 2 and Note 3 to entry have been removed.]

3.6.3
coverage probability
probability that the set of true quantity values of a SRS/SRSS measurement information is contained within a specified coverage interval

Note 1 to entry: The coverage probability is also termed "level of confidence", see ISO/IEC Guide 98-3:2008/Supplement 1).

[SOURCE: ISO/IEC Guide 99:2007, 2.37, modified – The definition has been changed to align to the use of this document, note 1 to entry has been changed and note 2 to entry has been removed.]

3.6.4
confidence information
safety related probability measure that supplements a measurement information or a decision information of an SRS/SRSS

Note 1 to entry: Confidence information cover coverage probability and coverage interval used if SRS/SRSS provides measurement information and decision probability if SRS/SRSS provide decision information.

3.6.5
decision probability
probability that the decision information is correct

3.6.6
digital signal
discretely-timed signal in which information is represented by a finite number of well defined discrete values that one of its characteristic quantities may take in time

[SOURCE: IEC 60050-702:1992, 702-04-05]

3.6.7
binary digital signal
binary signal
digital signal in which each signal element has one of two permitted discrete values

[SOURCE: IEC 60050-704:1993, 704-16-03]

3.6.8
***n*-ary digital signal**
***n*-ary signal**
digital signal in which each signal element has one of n permitted discrete values

[SOURCE: IEC 60050-704:1993, 704-16-05]

3.6.9
serial digital transmission
serial transmission
successive transmission of signal elements over a single path between two points

[SOURCE: IEC 60050-704:1993, 704-16-27]

3.6.10
parallel digital transmission
parallel transmission
simultaneous transmission of a group of signal elements over the appropriate number of parallel paths between two points

[SOURCE: IEC 60050-704:1993, 704-16-28]

3.6.11
fault reaction function
function that is initiated when a fault within an SRS/SRSS is detected by an SRS/SRSS diagnostic function

3.6.12
fault response time
maximum time between initiation of the SRS/SRSS signal to initiate the fault reaction function and achievement of an appropriate safety related information provided at the output unit

3.6.13
decision information
information which represents the decision performed in the SRS/SRSS of a respective variable quantity

Note 1 to entry: An example is a decision representing the entrance of an object in a safety related zone resulting in a switching signal.

Note 2 to entry: A respective variable quantity could be the properties of the object or environmental information.

3.6.14
SRS/SRSS measurement information
information which represents the respective variable quantity

Note 1 to entry: An example is the location of an object in a sensing zone provided as digital n-ary output signal.

3.7 Test

3.7.1
acceptance test
contractual procedure to demonstrate, to the customer, that acceptance criteria are met

[SOURCE: IEC 60050-192:2015, 192-09-03]

3.7.2
endurance test
procedure carried out to investigate how the properties of the item are affected by the duration or repeated application of stated stresses

[SOURCE: IEC 60050-192:2015, 192-09-07, modified – The note has been removed.]

3.7.3
field test
test carried out under user operational conditions

Note 1 to entry: The operating, environmental, maintenance and measurement conditions present at the time of the test may be monitored or recorded.

[SOURCE: IEC 60050-192:2015, 192-09-06]

3.7.4
laboratory test
test made under prescribed and controlled conditions that may or may not simulate field conditions

[SOURCE: IEC 60050-192:2015, 192-09-05]

3.7.5
maintenance test
test carried out periodically on an item to verify that its performance remains within specified limits, after having made certain adjustments, if necessary

[SOURCE: IEC 60050-151:2001, 151-16-25]

3.7.6
qualification test
procedure to verify conformance to the requirements of a specification

Note 1 to entry: A qualification test is generally performed before starting production of an item on a larger scale.

[SOURCE: IEC 60050-192:2015, 192-09-04]

3.7.7
routine test
test made on each individual item during or after manufacture

Note 1 to entry: A routine test is performed before supplying.

3.7.8
simulation test
test that imposes anticipated environmental and operating stresses of intended use

Note 1 to entry In practice, the test conditions only approximate to the true conditions of use, the accuracy of their reproduction being known as the degree of simulation.

[SOURCE: IEC 60050-192:2015, 192-09-18]

3.7.9
system test
test of a complete system to detect instances of non-conformity with the respective functional specification

Note 1 to entry: System test is mainly for verification (192-01-17), but may include some validation (192-01-18).

[SOURCE: IEC 60050-192:2015, 192-09-25]

3.7.10
test
determination according to requirements for a specific intended use or application

Note 1 to entry: If the result of a test shows conformity, it can be used for purposes of validation.

[SOURCE: ISO 9000:2015, 3.11.8]

3.7.11
type test
test of one or more devices under test made to a certain design to show that the design meets certain specifications

[SOURCE: IEC 60050-411:1996, 411-53-01, modified – The word "machines" has been replaced by "devices under test".]

3.8 User groups

3.8.1

integrator

entity who integrates an SRS and/or SRSS into an SCS and/or machinery or an SRS into an SRSS.

Note 1 to entry: The integrator may be a manufacturer, assembler, engineering company or the user.

Note 2 to entry: The integrator in sense of this document might be a manufacturer of an SRSS, SCS or machinery.

Note 3 to entry: Originally, the integrator is defined in ISO 11161 as "the entity who designs, provides, manufactures or assembles an integrated manufacturing system and is in charge of the safety strategy, including the protective measures, control interfaces and interconnections of the control system". It is changed in this document respectively to cover the relevant steps of integration up to integrated manufacturing system which is covered by the definition of machinery.

3.8.2

supplier

SRS/SRSS supplier

role in supply chain activities of organizations moving a product or service and corresponding information for use to customer and finally to the operator

Note 1 to entry: Supply chain activities involve the transformation of natural resources, raw materials, components and corresponding information into a finished product that is delivered to the end customer organisation.

Note 2 to entry: Supplier in the sense of this document might be manufacturer of an SRS, SRSS or machinery using SRS/SRSS.

3.8.3

user

SRS/SRSS user

addressed group or person at customer side organization

Note 1 to entry: A user might be the integrator, machinery manufacturer or operator.

3.9 Verification and validation

3.9.1

failure modes and effects analysis

FMEA

qualitative method of analysis that involves the study of possible failure modes and faults in sub items, and their effects at various indenture levels

Note 1 to entry: The term "fault mode and effects analysis" in IEC 60050-191:1990 (now withdrawn; replaced by IEC 60050-192:2015) is deprecated, since a fault (192-04-01) is a state and cannot logically have a mode, whereas a failure mode (192-03-17) is a change of state.

[SOURCE: IEC 60050-192:2015, 192-11-05, modified – The used term "DEPRACATED: fault mode and effects analysis" has been removed.]

3.9.2

fault tree analysis

FTA

deductive analysis using fault trees

Note 1 to entry: See also fault tree (192-11-07).

[SOURCE: IEC 60050-192:2015, 192-11-08]

3.9.3
formal design review
independent, documented examination of a design and its requirements to assess the design's ability to meet specified and implied requirements of the item concerned

Note 1 to entry: In this context, "design" includes requirements, specifications, drawings, and supporting documentation.

Note 2 to entry: See IEC 61160 for more detail on design review practices.

[SOURCE: IEC 60050-192:2015, 192-12-07]

3.9.4
inspection
examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements

Note 1 to entry: Inspection of a process may include inspection of persons, facilities, technology and methodology.

[SOURCE: ISO/IEC 17000:2004, 4.3]

3.9.5
life cycle
series of identifiable stages through which an item goes, from its conception to disposal

EXAMPLE A typical system lifecycle consists of: concept and definition; design and development; construction, installation and commissioning; operation and maintenance; mid-life upgrading, or life extension; and decommissioning and disposal.

Note 1 to entry: The stages identified will vary with the application.

[SOURCE: IEC 60050-192:2015, 192-01-09]

3.9.6
prediction
computation process used to obtain the predicted value of a quantity

[SOURCE: IEC 60050-192:2015, 192-11-01]

3.9.7
reliability model
mathematical model used for prediction or estimation of reliability measures

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

Note 2 to entry: Modelling techniques can be applied to other dependability characteristics, such as maintainability and availability.

[SOURCE: IEC 60050-192:2015, 192-11-02]

3.9.8
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry The objective evidence needed for a verification can be the result of an inspection (3.11.7) or of other forms of determination (3.11.1) such as performing alternative calculations or reviewing documents (3.8.5).

Note 2 to entry: The activities carried out for verification are sometimes called a qualification process (3.4.1).

Note 3 to entry: The word "verified" is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.12]

3.9.9
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Note 1 to entry: The objective evidence needed for a validation is the result of a test or other form of determination such as performing alternative calculations or reviewing documents

Note 2 to entry: The word "validated" is used to designate the corresponding status.

Note 3 to entry: The use conditions for validation can be real or simulated.

[SOURCE: ISO 9000:2015, 3.8.13]

4 Lifecycle and interconnection to safety-related electrical control systems (SCS)

4.1 General

A safety-related sensor (SRS) (see Figure 2 and Figure 3) or a safety-related sensor system (SRSS) (see Figure 4) used as a protective measure shall perform function(s) in accordance with 5.2.

An SRS consists, in minimum, of

- a sensing unit,
- a processing unit, and
- an output unit (input unit is optional).

An SRSS consists of at least two SRS in combination with processing unit and output unit (input unit is optional).

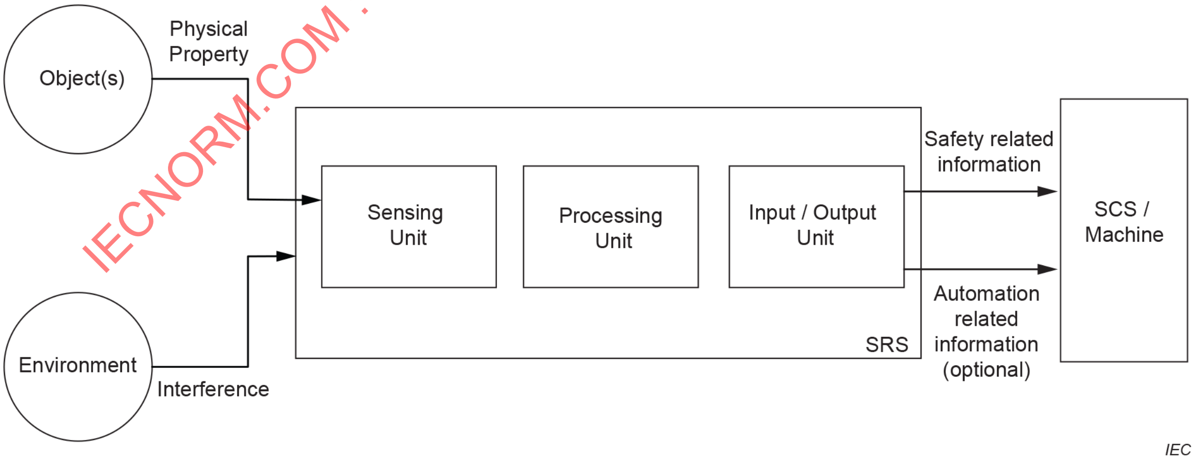


Figure 2 – Example 1 of SRS architecture

NOTE 1 An SRS can be constructed in a way that safety-related and automation-related functions are performed in separate or common sensing, processing and output unit.

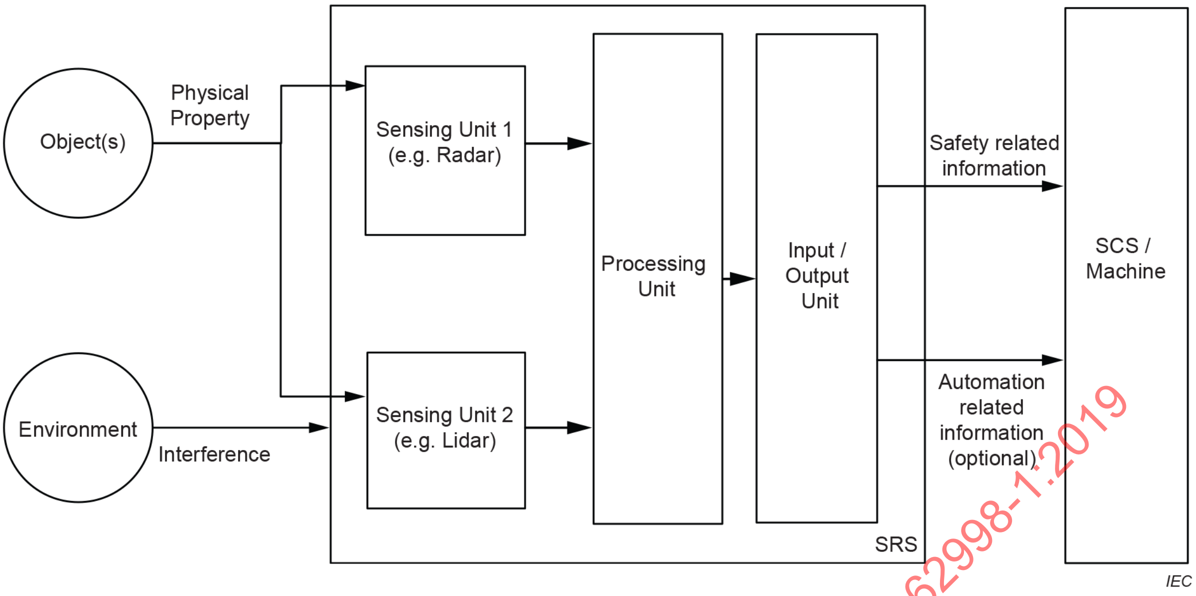

Object(s)
Physical Property
Environment
Interference
Sensing Unit 1 (e.g. Radar)
Sensing Unit 2 (e.g. Lidar)
Processing Unit
Input / Output Unit
SRS
Safety related information
Automation related information (optional)
SCS / Machine
IEC

Figure 3 – Example 2 of SRS architecture

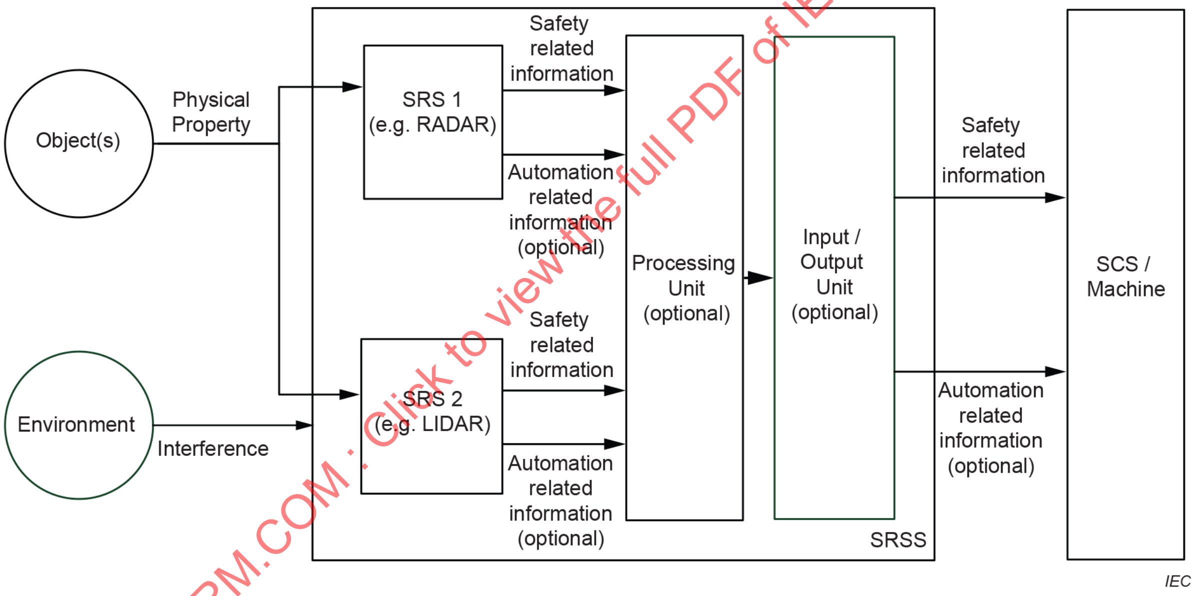

Object(s)
Physical Property
Environment
Interference
SRS 1 (e.g. RADAR)
SRS 2 (e.g. LIDAR)
Safety related information
Automation related information (optional)
Safety related information
Automation related information (optional)
Processing Unit (optional)
Input / Output Unit (optional)
SRSS
Safety related information
Automation related information (optional)
SCS / Machine
IEC

Figure 4 –Example of SRSS architecture

The sensing unit performs the sensing function by collecting information on physical properties of object(s) and/or environmental influences and provides it as input to the processing unit.

NOTE 2 The sensing unit can contain an emitting element or not.

The processing unit performs the processing function by processing information generated by the sensing unit in order to produce safety related information.

NOTE 3 The processing unit can be analog and/or digital.

The input/output unit

– is connected to a SCS/machine,

– will provide safety related information,

– can receive safety related information, and

– can provide automation related information.

If a safety related communication network is used at the input/output unit, it shall fulfil the requirements of applicable standards (e.g. for functional safety field bus in accordance with IEC 61784-3).

The manufacturer of an SRS/SRSS shall define appropriate technical and organisational measures in accordance with this document to achieve the systematic capabilities over the life cycle, taking into consideration all phases for the life cycle as defined in standards for functional safety of SCS or all of the following:

– hazard and risk analysis;

– design and development phase;

– integration and installation phase;

– operation, maintenance and modification phase.

Documentation of SRS/SRSS is assumed to be part of SCS documentation.

NOTE 4 SRS/SRSS safety requirement specification is part of the SCS safety requirement specification.

NOTE 5 The term "documentation" applies not only to documents in the traditional sense, but also to concepts such as data files and database information.

4.2 Hazard and risk analysis

4.2.1 General

Hazard and risk analysis shall be used to

– identify potential hazards caused by the SRS/SRSS, and

– identify the required level of safety performance (e.g. PL, SIL or $\mathrm{SIL}_{\mathrm{cl}}$) as a result of risk analysis of the application.

The interconnection to risk analysis in accordance with the application in the field of machinery as shown in Figure 5 should be done in advance of starting the SRS/SRSS design and development process. The results are an essential part of the safety requirement specification. During the SRS/SRSS design and development process, the hazards produced by the SRS/SRSS shall be identified and appropriate measures shall be added to the safety requirement specification. The information for use shall be provided with the SRS/SRSS for the respective user group(s).

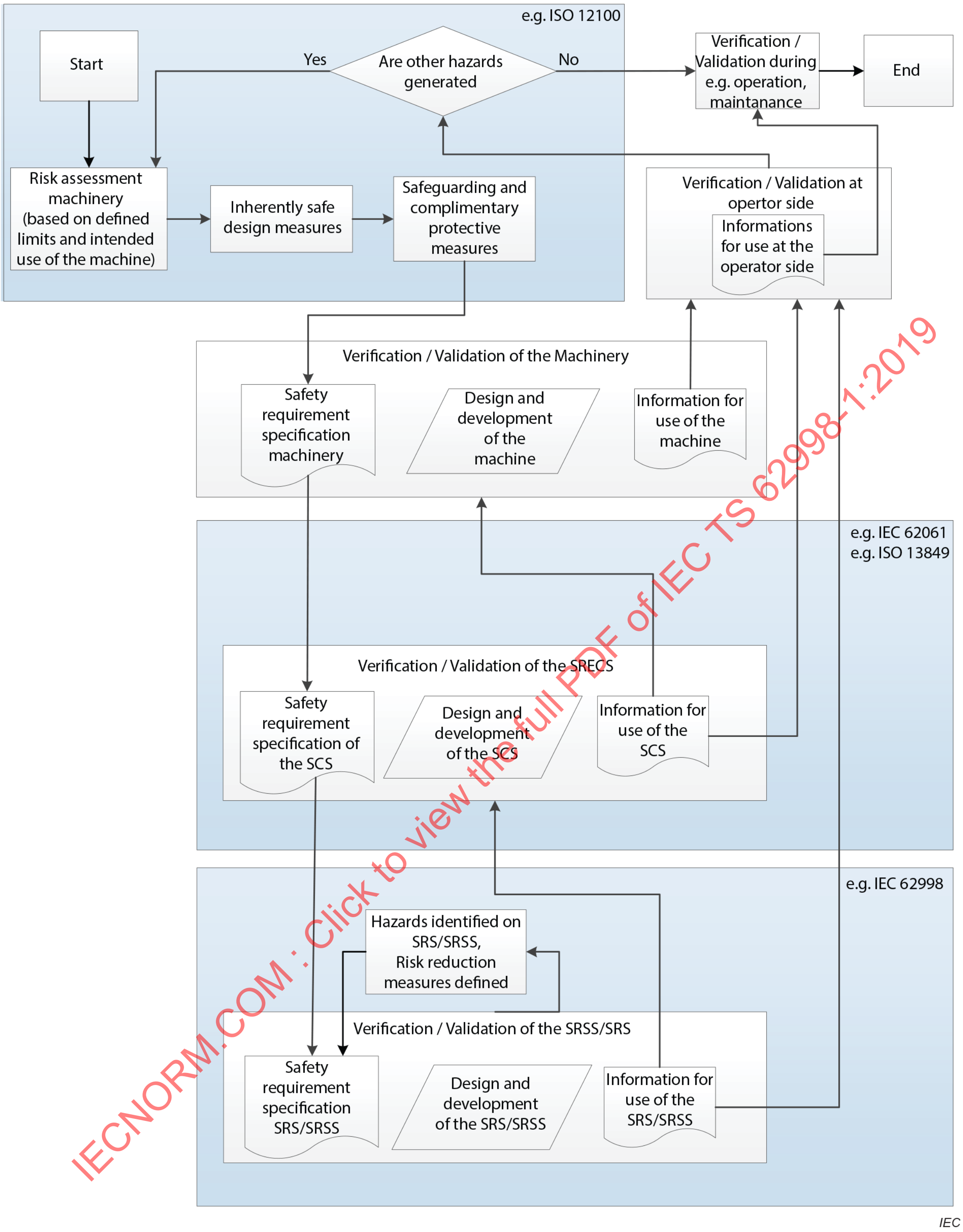

e.g. ISO 12100
Start
Yes
Are other hazards generated
No
Verification / Validation during e.g. operation, maintanance
End
Risk assessment machinery (based on defined limits and intended use of the machine)
Inherently safe design measures
Safeguarding and complimentary protective measures
Verification / Validation at opertor side
Informations for use at the operator side
Verification / Validation of the Machinery
Safety requirement specification machinery
Design and development of the machine
Information for use of the machine
e.g. IEC 62061
e.g. ISO 13849
Verification / Validation of the SRECS
Safety requirement specification of the SCS
Design and development of the SCS
Information for use of the SCS
e.g. IEC 62998
Hazards identified on SRS/SRSS, Risk reduction measures defined
Verification / Validation of the SRSS/SRS
Safety requirement specification SRS/SRSS
Design and development of the SRS/SRSS
Information for use of the SRS/SRSS
IEC

Figure 5 – Interconnection of an SRS/SRSS into hazard and risk analysis

4.2.2 Hazard caused by SRS/SRSS

4.2.2.1 General

The manufacturer shall analyse potential hazards caused by the SRS/SRSS and take measures to reduce the risk down to a tolerable risk in accordance with the respective standards.

NOTE 1 Hazards caused by the SRS/SRSS can arise, for example from the emission of optical radiation, emission of ultrasonic waves, exposure to ionizing radiation.

NOTE 2 Provisions for protection against hazardous electromagnetic emissions are given in relevant standards or regulations (see for example EN 50499, EN 50527 (all parts) and EN 50364; for ultrasonic technologies, see for example ISO 16148).

The result shall be documented.

4.2.2.2 Optical radiation hazards

Protection against hazardous coherent radiation shall be achieved in accordance with IEC 60825-1.

Protection against hazardous incoherent radiation shall be achieved in accordance with IEC 62471.

4.2.2.3 Electrical hazards

Protection against electrical shock shall be achieved in accordance with IEC 60204-1 or IEC 61010-1.

4.2.3 Required SRS/SRSS performance class

A risk analysis and risk reduction process in accordance with standards relevant for the intended use shall be conducted. If risk reduction is achieved by safety related control systems, the intended risk reduction shall be specified on basis of the output information of the overall risk reduction process. The required level of safety performance (e.g. PL, SIL or $\mathrm{SIL}_{\mathrm{cl}}$) of the safety related control system and the corresponding SRS/SRSS performance class (in accordance with 4.3) to achieve the intended risk reduction shall be identified using one of the following approaches:

- required safety performance for safety related control systems in accordance with specific machine type C standards;
- required safety performance of safety related control systems for the intended risk reduction as defined in generic or sector specific functional safety standards (e.g. ISO 13849 (all parts); IEC 62061; IEC 61508 (all parts), ISO 26262 (all parts), ISO 25119 (all parts)).

NOTE 1 The intended use is usually summarized as the "application". The application can be for example a specific type of machine, a general application as electrical equipment within a sector like machinery, or the general use as part of safety related control system as described in IEC 61508 (all parts).

NOTE 2 For safety of industrial machinery, the fundamental International Standard is ISO 12100. Machinery manufacturers can work through the risk assessment and risk reduction process described in ISO 12100 to identify hazards, estimate risks and reduce risks adequately. The relationship of ISO 12100 and type-B and type-C standards is discussed in ISO TR 22100-1; the relation of ISO 13849-1 and ISO 12100 is discussed in ISO TR 22100-2.

4.3 Correspondence SRS/SRSS performance class

The SRS/SRSS performance class shall be used following the procedures starting from Clause 5.

The correspondence of required level of safety performance and minimum required SRS/SRSS performance class is regarded as shown in Table 1.

Table 1 – Correspondence between level of safety performance and minimum required SRS/SRSS performance class

	SRS/SRSS performance class A	**SRS/SRSS performance class** B	**SRS/SRSS performance class** C	**SRS/SRSS performance class** D	**SRS/SRSS performance class** E	**SRS/SRSS performance class** F
ISO 13849	PL_{a}	PL_{b}	PL_{c}	PL_{d}	PL_{e}	
IEC 62061			SIL_{cl} 1	SIL_{cl} 2	SIL_{cl} 3	
IEC 61508			SIL 1	SIL 2	SIL 3	SIL 4
To be determined[a]						

NOTE 1 There are already a lot of different performance classes defined which could lead to confusion at the end user side. The existing Type in accordance with IEC 61496 definition is not used because the design specific approach should be clearly distinguished to the generic approach following this document.

NOTE 2 Correspondence to the different levels of safety performance of the safety related electrical, electronic and software parts of an SRS/SRSS is due to the fact that provided risk reduction is limited also by the systematic capabilities (for example environmental influences, EMC, detection capability and sensing technology).

[a] Table 1 establishes a correspondence between the performance class of this document and the level of safety performance of ISO 13849 (all parts), IEC 62061 and IEC 61508 (all parts). Nevertheless, additional links can be established in future to other level of safety performance schemes as for example the Agriculture PL of ISO 25119 (all parts) and the ASIL of ISO 26262 (all parts).

The defined SRS/SRSS performance class (e.g. SRS performance class B) and the level of safety performance (e.g. PL, SIL or SIL_{cl}) shall be stated by the supplier within information for use. The information for use shall state unambiguously that

- the element /subsystem description and level of safety performance is in accordance with a referenced standard for safety related control systems, and
- the SRS/SRSS performance class is in accordance with this document used for examination of systematic capabilities.

EXAMPLE Sensor Subsystem SIL 2 in accordance with IEC 62061. SRS performance class D in accordance with this document used for examination of systematic capabilities.

5 Design and development phase

5.1 General

The SRS/SRSS shall be designed and developed covering in minimum the following items:

- determination of the intended use;
- definition of required SRS/SRSS functions in accordance with 5.2;
- documentation of resulting safety related requirements in a safety requirement specification;
- design of safety related electrical, electronic and software in accordance with stated level of safety performance and referenced standard (see 4.3);
- design analysis supported by simulation as defined in 5.3 and 5.4.

NOTE IEC 61508-1:2010, 7.6.2.11, requires that for an E/E/PE safety-related system implementing a SIL 4 safety function, i.e. a performance class F SRS/SRSS, there is a reconsideration of the application to determine if any of the risk parameters can be modified so that the requirement for a SIL 4 safety function is avoided.

5.2 SRS/SRSS functions

For all SRS/SRSS performance classes, the SRS and/or SRSS functions shall be

- defined by the manufacturer and decomposed into functions in accordance with general description of Table 2, and
- stated in the information for use.

The safety related functions shall be

- performed under the specified environmental conditions,
- performed at limit of use as defined by the manufacturer, and
- documented within the safety requirement specification.

Table 2 – Functions of an SRS/SRSS as applicable

Functions	General description
SRS/SRSS function	Time dependent determination of defined object(s): • with defined physical properties, • in a defined application, • under environmental conditions, and provision of an appropriate output information.
Safety related function	Parts of SRS/SRSS function detecting safety related objects for which malfunction or improper performance would lead to a degradation of stated detection capability beyond the limits stated in this document resulting in a failure to danger.
Automation related function	Parts of SRS/SRSS function detecting objects for which malfunction or improper performance does not result in a failure to danger.
Hazardous object function	Parts of safety related function detecting safety related objects being a source of hazard when they enter into or are present in a safety related zone.
Person detection function	Parts of safety related function detecting safety related objects representing persons or parts of persons when they enter into or are present in a safety related zone.
NOTE The functions in accordance with Table 2 are requested during design and development and used in the applications to identify which parts of a safety function, for example of a machine, is provided by an SRS/SRSS. Further information on decomposition of a safety function is given in Annex C.	

5.3 Design analysis

For all SRS/SRSS performance classes, the design of the SRS/SRSS shall be analysed for

- failure to danger in safety related functions under environmental conditions as defined in 5.8.3.3,
- normal operation under environmental conditions defined in 5.8.3.4,
- type and combination of physical properties of the safety related object in relation to the sensing technology, and
- limits of detection capability and dependability of it.

NOTE 1 Methods for design analysis as part of verifcation are defined in 8.4.

NOTE 2 Where algorithms are used for detection, they are part of the analysis.

For SRS/SRSS performance classes C, D, E and F, the design of the SRS/SRSS shall be analysed for failure to danger of the safety related function if automation related function is performed.

5.4 Simulation

For SRS/SRSS performance classes D, E and F, the design analysis shall contain a simulation to identify that the safety related function of the SRS/SRSS is performed

- under tolerance conditions of components,

- over the mission time stated, and
- at the limits of use as defined by the manufacturer.

The simulation shall be executed by the manufacturer using in minimum

- deterministic and/or probabilistic calculations,
- data from component suppliers,
- data from ongoing qualification tests, and
- data from investigations during design and development.

The simulation shall be verified by type test.

NOTE More detailed information for generation and application of simulation used for analysis of an SRS/SRSS is given in Annex D.

5.5 Sensing zone(s)

The supplier shall provide information on the sensing zone(s) if applicable.

An object or objects in accordance with 5.8.2.2 and 5.8.2.3 at any position inside the sensing zone shall not result in a degradation of the detection capability inside the safety related zone or shall lead to appropriate safety related information at the output unit.

5.6 Safety related zone

The supplier shall provide information on relevant parameters of the safety related zone(s).

An object/objects in accordance with 5.8.2.2 and 5.8.2.3 at any position inside the safety related zone shall

- be detected, and
- lead to an appropriate safety related information at the output unit.

5.7 Automation related zone

The supplier shall provide information on automation related zones, if applicable.

NOTE Automation related functions for purpose of quality control or process control can be performed inside an automation related zone.

For SRS/SRSS performance classes C, D, E and F, an object or objects in accordance with 5.8.2.4 at any position inside the automation related zone

- shall not lead to a failure to danger of the safety related function, and
- can lead to an automation related information at the output unit.

5.8 Detection capability and dependability

5.8.1 General

The detection capability and the dependability of the detection capability of an SRS/SRSS shall be analysed and tested taking into account the following:

- object classes and physical properties as defined in 5.8.2;
- limits of use;
- SRS/SRSS performance class;
- foreseeable misuse;
- environmental influences as defined for failure to danger in 5.8.3.3 considering dependability items:

- integrity;
- reliability;
- safety.

– environmental influences as defined for normal operation in 5.8.3.4 considering dependability items:

- availability;
- robustness.

For SRS/SRSS performance classes A and B, appropriate testing can be sufficient and analysis may be omitted.

5.8.2 Object classes and physical properties

5.8.2.1 General

The objects shall be defined by the manufacturer and shall be detected based on their physical properties used to perform the functions in accordance with Table 2.

Objects shall be defined as:

– objects used to perform the person detection function;

– objects used to perform the hazardous object function;

– objects used to perform the automation related function.

The physical properties used for the detection of safety related objects shall be:

– representative for the safety related objects as defined in the safety requirements specification by the manufacturer;

– appropriate for the sensing technology used to perform person detection function and the hazardous object function in accordance with Table 2.

NOTE 1 The physical properties of an object can include, but are not limited to: absorption (physical), absorption (electromagnetic), area, capacitance, density, dielectric, ductility, elasticity, electric charge, electrical conductivity, electrical impedance, electric field, emission, flow rate, fluidity, frequency, hardness, inductance, Intrinsic impedance, Intensity, irradiance, length, location, luminance, luminescence, malleability, magnetic field, opacity, permeability, permittivity, radiance, reflectivity, strength, temperature, thermal conductivity, velocity, volume.

NOTE 2 State of the art can be considered for the definition of physical property limits (e.g. application standards, sensor related product standards).

The limits of the physical properties within which the SRS-SRSS function is performed shall be defined and be provided within the information for use.

5.8.2.2 Persons and related properties

If applicable, the manufacturer shall specify the physical properties used for person detection and limits of the physical properties within which the person detection function is performed.

The limits defined for the physical properties shall be used for design and development.

Property length, area and volume of adult persons or parts of adult persons shall be in accordance with ISO 7250 (all parts).

NOTE 1 Within ISO 7250 (all parts), only adult persons are represented.

If the SRS/SRSS is intended to be used for detection of children:

– the range of considered age under 14 years shall be defined by the manufacturer;

- the age specific behaviour and development as listed in Annex C and Annex D of CEN/CENELC Guide 14 shall be taken into account;
- the size(s) representing the body or parts of body of a child shall be defined by the manufacturer and Annex E should be considered.

Property reflectivity shall be derived from the properties of skin and of fabric.

The dependence of wavelength shall be taken into account if radiation is used to perform the sensing function.

NOTE 2 Further information on reflectivity can be given in sources including standards (e.g. IEC 61496-3, ANSI/ITSDF B56.5:2012, ISO 15622, ISO 18497).

Unless specifically required otherwise by the intended use of operation, diffuse reflection shall be assumed.

Unless specifically required otherwise by the intended use, the velocity representing walking of adult persons shall be assumed between 0 mm/s and 1 600 mm/s.

NOTE 3 1 600 mm/s for velocity is in accordance with intended use of an industrial environment as defined in ISO 13855. Typically organizational measures are set in place to inform workers that running is prohibited.

Unless specifically required otherwise by the intended use the acceleration of adult persons shall be assumed to be between 0 mm/s^2 and 2 000 mm/s^2.

NOTE 4 2 000 mm/s^2 is the acceleration of an adult person initiating normal walking speed of 1 600 mm/s according to [1].

NOTE 5 Velocities and acceleration for running person is different.

If applicable, property velocity and acceleration of children shall be defined by the manufacturer taking into account the behaviour as referenced in Annex E.

5.8.2.3 Hazardous object

If applicable, the manufacturer shall specify the physical properties used for hazardous object detection and limits of the physical properties within which the hazardous object function is performed.

5.8.2.4 Automation object

If applicable, the manufacturer shall specify objects used to perform automation related functions for SRS/SRSS performance class C, D, E and F.

NOTE Specification is used to inform under which assumptions design and development was made to investigate the influence of automation objects on safety related functions of the SRS/SRSS.

5.8.3 Environmental influences

5.8.3.1 General

The manufacturer shall specify the environmental influences that can result in a degradation of the dependability of an SRS/SRSS.

The potential degradation by specified environmental influences shall be analysed taking into account the following:

- intended use;
- sensor technologies of SRS/SRSS;
- physical properties of safety related object(s).

5.8.3.2 Conditions and limits

The manufacturer of the SRS/SRSS shall identify environmental conditions and limits taking into account the intended use. Environmental parameters and severities shall be selected from IEC 60721 (all parts) considering the following items but not limited to:

a) indoor and/or outdoor use (sheltered or not);
b) stationary operation and/or mobile operation;
c) temperature and humidity;
d) precipitation (rain, hail or snow) and wind;
e) pressure (of surrounding air, water, etc.);
f) solar radiation and thermal radiation;
g) condensation and icing;
h) fog, dust, sand and salt mist;
i) vibration and shocks;
j) fauna and flora (e.g. mould growth);
k) chemical influences;
l) electrical and electromagnetic influences;
m) mechanical load;
n) sound.

NOTE 1 Annex F shows examples of how the listed environmental conditions can be applied.

An application specific standard for machinery may give detailed requirements for some or all of the items listed above.

Examples of sector or machine type specific standards that specify environmental requirements are given in Table 3.

Table 3 – Standards that contain environmental requirements

Standard	Sector/specific machine type
IEC 60654-1	Industrial process measurement and control equipment – Operating conditions
ISO 15003	Agricultural engineering — Electrical and electronic equipment — Testing resistance to environmental conditions
EN 50125-1	Railway applications – Environmental conditions for equipment – Part 1: Rolling stock and on-board equipment
ISO 15998	Earth-moving machinery — Machine control systems (MCS) using electronic components — Performance criteria and tests for functional safety
IEC 60721-3-3	Classification of environmental conditions – Part 3-3: Classification of groups of environmental parameters and their severities – Stationary use at weather protected locations
IEC 60721-3-4	Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 4: Stationary use at non-weather protected locations
IEC 60721-3-5	Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 5: Ground vehicle installations
IEC 60721-3-6	Classification of environmental conditions – Part 3: Classification of groups of environmental parameters and their severities – Section 6: Ship environment

The manufacturer shall specify for all relevant environmental influences the limits for failure to danger condition and for normal operating condition.

NOTE 2 The environmental conditions are used for analysis and testing and to describe the limits of use. Limits of use in type and range are for example operation temperature 0° to 50°C.

NOTE 3 It is possible that some environmental conditions are not described in some standards. Public available documents could be used to investigate their influence on sensing technology. One example for snow is provided in [2].

5.8.3.3 Failure to danger

There shall be no failure to danger due to a loss of the detection capability in the safety related functions of the SRS/SRSS beyond the limits specified in Table 4 in presence of

– environmental conditions relevant for the intended use according to the analysis of 5.8.3.1, and

– application relevant objects, including safety related object(s), anywhere inside the safety related zone.

Table 4 is intended to provide generic constraints and shall only be used in conjunction with the relevant text of 5.8.3.3. Analysis at the application level considering the relevant environmental conditions shall be conducted to determine if the expected rate and duration of the occurrence of loss of the detection capability and the expected demand are likely to result in a foreseeable hazardous situation. If this is the case, the limits in Table 4 shall not be used as a constraint and further measures shall be applied.

EXAMPLE 1 Where any loss or degradation of the detection capability would immediately result in a hazardous situation.

EXAMPLE 2 If the environmental influence which causes the loss or degradation of the detection capability also increases the level of risk, for example falling snow which degrades the detection capability also increases stopping distance of a mobile hazard.

The manufacturer shall analyze the influence of relevant environmental conditions on the detection capability using

– simulation(s) and/or test(s) of the influences in accordance with 5.8.3.2 under which a loss of detection can occur, and

– determination of the quantitative limits of influences that result in a loss of the detection capability.

The manufacturer shall document during design and development the results of analysis, determined limits and compliance with Table 4.

Table 4 – Limits for failure to danger condition (loss of the detection capability) due to environmental interference for high demand mode

SRS/SRSS performance class	Maximum accumulated duration of failure to danger per year
A	1 h
B	5 min
C	1 min
D	5 sec
E	0,5 sec
F	Response time

NOTE 1 Maximum values are defined due to the fact that sporadic effects under environmental conditions are in line with probabilistic requirements for integrity of generic standard ISO 13849-1. The limits for the duration of failure to danger derive from PFH_D-values being interpreted as fraction of the year. Table G1 illustrates the connection.

If the response time of an SRS/SRSS is longer than the maximum duration specified in Table 4, it replaces the corresponding limit value in the table. No SRS/SRSS is required to provide detection faster than its specified response time. If the duration of failure to danger is limited to the response time of an SRS/SRSS, there is no limitation concerning the accumulated duration.

If it is not possible for the manufacturer to ensure that the duration of a failure to danger due to a loss of detection capability stays below the limits specified in Table 4 the manufacturer shall give a justification by analysis why the limits of Table 4 are not achievable with adequate measures in the SRS/SRSS and proceed in accordance with one of the additional approaches as illustrated in Figure G.2 by applying one or more of the following:

- define limitations in use to prevent failure to danger under specific environmental conditions and provide appropriate additional information for use; or
- determine that limits in accordance with Formula G.1 are fulfilled for a specific demand rate and give appropriate additional information for use, or
- determine type and value of the degradation of the detection capability of the SRS/SRSS and provide appropriate additional information for use.

The results of justification, determination and defined limits shall be documented.

NOTE 2 Appropriate provided information to the user can contain measures to reduce the coverage/decision probability or prevent a failure to danger under the relevant environmental influences (e.g. installation warning information, field test, alternative measures for appropriate risk reduction,) or consequences if these limits are not achieved in the application (see Annex G).

5.8.3.4 Normal operation

The manufacturer shall analyse for each relevant environmental influence according to 5.8.3.2 up to which limits the SRS/SRSS provides normal operation.

For all relevant environmental influences according to 5.8.3.2, the manufacturer of the SRS/SRSS shall:

- prove normal operation under the specified limits by environmental tests according to IEC 60068 (all parts) and/or verified simulations;
- specify measures to reduce the detrimental effect of environmental influences on availability if achieved values are outside the limits as defined in the sSafety requirement specification;
- provide information to the user on the limits of normal operation of the SRS/SRSS;
- provide additional information on measures for the use of the SRS/SRSS outside the limits of normal operation if applicable.

EXAMPLE Measures could be:

- an output signal of the sensor that informs on excessive environmental influences leading to reduced availability or that triggers alternative operation states;
- alternative states of SRS/SRSS operation with degraded detection capability that are more robust to environmental influences. This is possible if the hazardous motion of the machine can be adapted accordingly (e.g. reduced speed of an AGV in heavy rain or snow at reduced sensor range).

Limits should be given predominantly by values, see example in Annex F.

NOTE Requirements in normal operation are defined to achieve availability and robustness resulting in an appropriate dependability. If normal operation is not achieved, there is an increased risk for bypassing the safety function.

5.9 User interface

5.9.1 General

The manufacturer shall define the type and performance of safety related user interface(s) inside the safety requirement specification.

Type and performance shall be sufficient to perform the safety related function for the intended use and shall content in minimum requirements on:

- mounting;
- safety related information (at input/output unit);
- organizational measures for risk reduction on user interface during life cycle (e.g maintenance test of detection capability).

NOTE This document does not deal with procedures on user interface as input for an SRS/SRSS for for example configuration or power supplies to take the SRS/SRSS into operation. The main goal of this document is to give guidance for the examination of the systematic capabilities.

The performance of the user interface shall be valid over the lifecycle and the supplier shall inform the user on all procedures (e.g. tests) during lifecycle of the SRS/SRSS taking into account:

- integration of safety related information into an safety related control system;
- taking into operation at the end user side;
- troubleshooting during operation;
- maintenance (in example replacement).

5.9.2 Mounting

The supplier shall inform the user about:

- restriction in mounting position of a sensing unit/SRS/SRSS (e.g. only top mounting);
- location of sensing zone(s) relative to mounting surfaces or reference point at the sensing unit/SRS/SRSS;
- location and limitations in mounting of sensing unit/SRS/SRSS;
- detection capability in an SRS/SRSS as a result of mounting;
- location and geometry of SRS/SRSS sensing zone(s);
- measures to prevent or monitor changes in mounting resulting in failure to danger (e.g. ground truth points, references, torque limits, form closures).

If brackets for mounting are provided by the supplier, these shall be used for type test and acceptance test as far as reasonable applicable.

5.9.3 Safety related information

5.9.3.1 General

The manufacturer shall define the safety related information provided by the SRS/SRSS (see Figure 6).

Safety related information are:

- result of determination of the presence of a physical property provided as a decision information; and/or
- value of a physical property provided as a measurement information; and
- their corresponding confidence information.

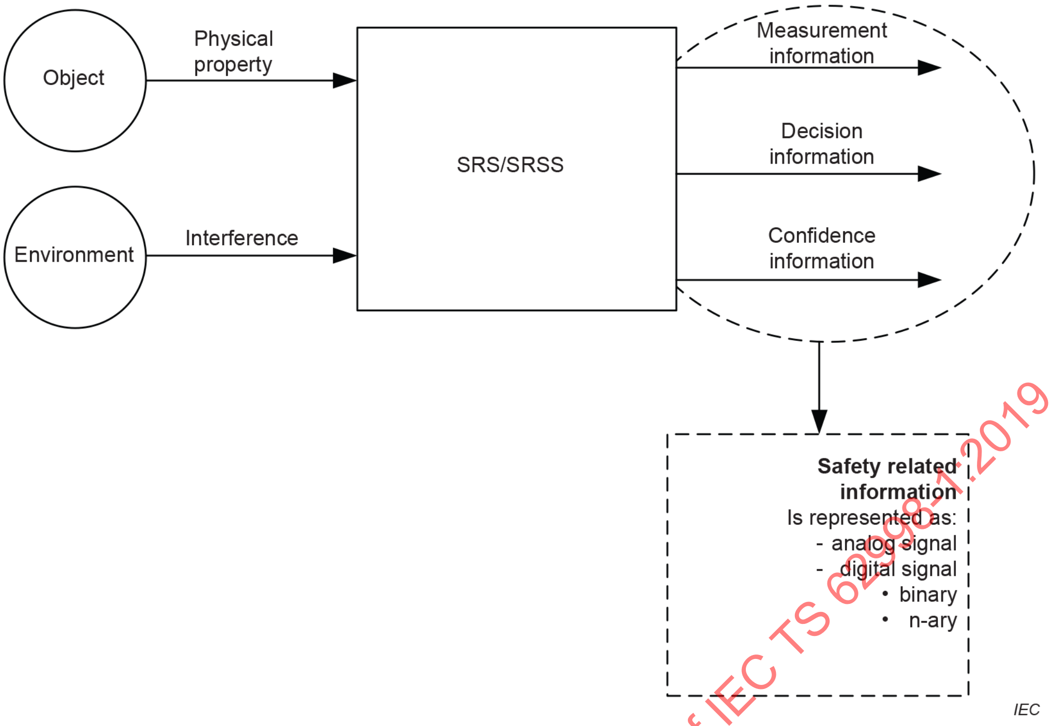


Figure 6 – Safety related information of an SRS/SRSS

The safety related information provided by the output unit of the SRS/SRSS shall be of one of the following signal types:

– analog; and/or

– digital binary or n-ary transmitted by a:

  - serial transmission path; and/or
  - parallel transmission path.

NOTE 1 The output unit can provide three types of electrical signals. Analog electrical signals (e.g. current, voltage), hybrid analog and digital electrical (e.g. current and HART protocol or binary switch and I/O link) or a digital output only (e.g. via fieldbus protocol, wired or wireless).

The signal to initiate the fault reaction function and its fault response time shall be specified and provided within the information for use for SRS/SRSS performance class C to F.

NOTE 2 Examples for signal to initiate the fault reaction function are given in Clause G.4.

5.9.3.2 Measurement, decision and confidence information

The manufacturer shall specify the measurement information, if applicable, and give appropriate information within the information for use.

NOTE 1 Measurement information can contain type and unit of measurement (e.g. distances in mm, temperature in Kelvin) and signal type and description of used signal at the output unit (e.g. binary digital signal, protocol for information transmission over serial transmission path).

The manufacturer shall specify the decision information, if applicable, and give appropriate information within the information for use.

NOTE 2 Decision information could contain decision criteria (object with defined size in defined area) and corresponding signal at the output unit (e.g. high signal in voltage if criteria is achieved and low level signal if criteria is not achieved).

The manufacturer shall specify confidence information for the safety related information. Confidence information shall cover:

– coverage probability and coverage interval if the SRS/SRSS provide measurement information; and/or

– decision probability if SRS/SRSS provide decision information.

Systematic faults and errors influence the stated confidence information. If errors can be compensated by, for example, calibration at user side, the corresponding measures should be defined in accordance with 6.3.

NOTE 3 Confidence information could be constant or variable over time.

NOTE 4 Confidence information could be provided as analog and/or digital signal at the output unit and/or within information for use.

NOTE 5 Coverage interval cannot be applied to decision information which is discrete.

The minimum required coverage probability and/or decision probability shall be in accordance with Table 5 or Formula (1).

Table 5 – Minimum required coverage probability/decision probability at high demand rate

SRS/SRSS performance class	A	B	C	D	E	F
Assumed high demand rate	1/24h	1/h	1/h	4/h	4/h	4/h
Coverage probability if measurement information is provided	>1-2,4* 10^{-3}	>1-1* 10^{-5}	>1-3* 10^{-6}	>1-2,5* 10^{-7}	>1-2,5* 10^{-8}	>1-2,5* 10^{-9}
Decision probability if decision information is provided	>1-2,4* 10^{-3}	>1-1* 10^{-5}	>1-3* 10^{-6}	>1-2,5* 10^{-7}	>1-2,5* 10^{-8}	>1-2,5* 10^{-9}
NOTE Equal values for coverage probability and decision probability are used in Table 5 because both would result in the same increase of risk.						

If an application specific demand rate will be applied instead of Table 5, following Formula (1) shall be applied.

$$P > 1 - \frac{L}{D} \qquad (1)$$

where

P is the coverage probability or decision probability;

L is the upper limit PFH corresponding to SRS/SRSS performance class;

D is the application specific demand rate.

NOTE 6 Upper limit of PFH can be taken from generic functional safety standards such as IEC 62061 or ISO 13849-1.

5.9.3.3 Response time

The time from a change of a measured physical property until the corresponding change of the safety related information provided at the output unit shall be specified.

There could be different response times if the SRS/SRSS provides confidence information, measurement information or decision information. The different response times should be defined unambiguously.

The manufacturer shall analyse that the specified safety related object with defined physical properties is detected within the response time within the specified limits of use.

NOTE Within limits of use, for example the dimension of safety related zone, the response time is defined to achieve detection of the object with a specific property (e.g. speed).

6 Integration and installation phase

6.1 General

The manufacturer of an SRS/SRSS shall define:

- measures for further integration of an SRS/SRSS into SCS to achieve the safety related function (e.g. test to be performed for verification of systematic capabilities and appropriate use of safety related information after integration), if applicable,
- measures for further integration of two or more SRS into an SRSS using fusion approach in accordance with 6.2, if applicable,
- measures for installation of an SRS/SRSS at user side to achieve the safety related function of an SRS/SRSS (e.g. need for inspection of right setting of safety related zones in respect to the mounting conditions), if applicable, and
- measures for calibration at user side to achieve the stated detection capability in accordance with 6.3, if applicable.

The supplier of an SRS/SRSS shall give appropriate information for integration and installation within the information for use.

6.2 Fusion of SRS into an SRSS

6.2.1 General

Fusion of two or more SRS into an SRSS is used to improve the limit of use compared to a single SRS.

Subclause 6.2 gives specific requirements to fusion of two or more SRS into an SRSS (Figure 4) by the user group SRS integrator into an SRSS (furthermore named SRSS integrator in 6.2).

Subclause 6.2 applies only if the physical property of a safety related object is the basis for fusion of two or more SRS into an SRSS within the limits of physical properties as defined for the SRS by the manufacturer and provided within the information for use by the supplier.

NOTE 1 6.2 does not apply to higher level functions like object recognition or classification or complex physical models.

NOTE 2 The integration of sensing units, SRS, SRSS and their relationship to sensor fusion is explained in more detail in Annex B (user groups) and Annex I (Examples of functions, safety related information and fusion).

NOTE 3 Combination of sensing units within an SRS is not covered in 6.2. Example for combinations of sensing units in an SRS (Figure 3) is a combination of different sensor technologies like LIDAR (light detection and ranging) sensing unit with Radar sensing unit. This is covered by the requirements as given for the SRS manufacturer.

NOTE 4 The user group integrator of SRS into an SRSS is assumed as being not as familiar with determination of SRS/SRSS detection capabilities as the manufacturer of an SRS/SRSS. The integrator is instructed by the information for use provided by the SRS (see Annex B – User groups).

NOTE 5 The user group integrator of SRS into an SRSS is assumed as being familiar with fusion of safety related information. Usually, integrators have competence in signal processing which is used for the fusion of safety related information.

The SRSS using 2 or more SRS shall be designed and developed covering at minimum the following items:

- determination of the intended use of the SRSS;
- definition of resulting SRSS functions under consideration of already defined SRS function;
- documentation of resulting safety related requirements in a safety requirement specification;
- design requirements of safety related hardware and software in accordance with stated level of safety performance (PL, SIL, or SIL_{cl}) in accordance with Table 1, if SRSS performance class is higher than SRS performance class (see 6.2.7);

The SRSS integrator shall:

- define limits of use of the SRSS using two or more SRS in accordance with 6.2.2;
- validate that each SRS is used within the limits of use as defined within the information for use as provided by the SRS supplier;
- verify improved limits of use (e.g. detection capability and safety related information) of the SRSS in accordance with 6.2.9;
- provide appropriate information for use of the SRSS and each SRS to the user.

6.2.2 Limits of use after fusion

The SRSS integrator shall define and document the limits of use of the SRSS considering:

- detection capabilities (see 6.2.3);
- sensing zones (see 6.2.4);
- dependability under environmental conditions (see 6.2.5);
- safety related information (see 6.2.6);
- SRS performance class(see 6.2.7);
- response time after fusion (see 6.2.8).

The SRSS integrator shall define and document the limits of use if the fusion of two or more SRS into an SRSS results in an improvement, in a degradation or in equal characteristics as defined for each SRS by the manufacturer.

NOTE 1 Aspects of the detection capability to be considered are for instance the object location, object size, response time or measurement accuracy. Improvements regarding the sensing zone could be an extension of the zone.

NOTE 2 Improvement of detection capability in an SRSS could be achieved by combination of 2 SRS sensing zone mounted on different positions resulting in one common sensing zone with reduced size. Finally, the limits of use could be improved from intended use point of view (see Figure I.1).

6.2.3 Detection capability after fusion

The SRSS integrator shall specify the resulting SRSS detection capability considering:

- detection capability of the SRS;
- limits of use of the SRS;
- physical properties used for detection by the SRS;
- possible interference effects between the SRS;
- alignment of SRS safety-related information.

NOTE 1 If more than one SRS simultaneously use probe radiation, such as illumination light or radar emission or emit electro-magnetic radiation, the detection capability of the SRSS could be impaired due to mutual interference of the SRS.

NOTE 2 Various aspects of detection capability such as position accuracy or response time rely on the exact alignment of SRS output data (for instance a coordinate offset or a timing offset can induce measurement error or inconsistencies in fused sensor data).

The SRSS integrator shall verify the resulting detection capability of the SRSS by test in accordance with 8.5 and shall additionally classify the test results in the report as "after fusion".

6.2.4 Sensing zone(s) after fusion

The SRSS integrator shall specify the resulting sensing zone(s) considering:

- sensing zone of the SRS as defined by the manufacturer;
- the specified detection capability of the SRS;
- limits of use of the SRS;
- interference effects between the SRS;
- mounting and relative orientation of the SRS;
- alignment of safety related information of the SRS.

The SRSS detection capability as defined by the SRSS integrator shall be ensured within the fused sensing zone(s).

NOTE Errors in mechanical alignment of mounting or alignment tolerances of the SRS safety-related information can have an effect on the fused sensing zones.

The SRSS integrator shall verify the specified sensing zones of the SRSS by test in accordance with 8.5 and shall additionally classify the test results in the report as "after fusion".

6.2.5 Dependability under environmental condition after fusion

The SRSS integrator shall specify the limits of all relevant environmental influences:

- regarding failure to danger of the SRS;
- regarding normal operation of the SRS.

The requirements given in 5.8.3.3 for no failure to danger due to a loss of the detection capability in the safety related functions of the SRS/SRSS shall be fulfilled except the requirement for analysis using simulation techniques.

NOTE Simulation cannot be used because the SRSS integrator usually does not have enough information on the sensor technologies used within an SRS.

The SRSS integrator shall specify for each environmental influence the limits where the SRSS provides no failure to danger taking into account the environmental limits for no failure to danger as defined by the SRS manufacturer.

The SRSS integrator shall specify for each environmental influence the limits where the SRSS provides normal operation taking into account the environmental limits for normal operation as defined by the SRS manufacturer.

6.2.6 Safety related information after fusion

The SRSS integrator shall specify logic functions performed in a processing unit of the SRSS and shall specify the safety related information provided by the SRSS considering:

- the measurement information of the SRS;

- the decision information of the SRS;
- the corresponding confidence information.

If the SRSS provides safety related information with an improved confidence as compared to the individual SRS, the improvement and the related confidence information of the SRSS shall

- be based on the confidence information of the SRS,
- take into account the detailed processing algorithm of the SRSS, and
- be ensured by appropriate methods (e.g. by propagation of errors calculation or by simulation).

NOTE 1 In general, fusion can be accomplished by a large variety of algorithms performed in the SRSS, for example using the central limit theorem, Kalman filters, Bayesian networks and many others. Some of these approaches require detailed knowledge to determine the resulting safety related information and the corresponding confidence information.

NOTE 2 For further information on error propagation see ISO/IEC Guide 98-1.

The fusion process of inconsistent SRS safety related information can lead to reduced SRSS confidence or degraded detection capability. The SRSS integrator shall analyse if and under which conditions inconsistencies can occur and how they affect the detection capability and confidence information.

The confidence information of an SRSS shall fulfil the requirements of Table 5 or Formula (1).

6.2.7 SRSS performance class after fusion

The SRSS integrator shall specify the resulting sensor performance class considering:

- sensor performance classes of each single SRS as defined by the manufacturer;
- limits of use of SRS as defined by the manufacturer;
- confidence information of SRS;
- diversity and/or redundancy of the SRS sensor technologies.

The maximum applicable SRSS performance class for the SRSS using fusion of safety related information of two SRS is given in Table 6 if:

- the SRSS provides safety-related information with increased dependability; and
- each SRS already provides the safety related information of the SRSS; and
- the SRS are mounted and/or configured such that a degradation of the performance of detection/measurement of one SRS (e.g. by environmental influences) is compensated by the other SRS.

Table 6 – Maximum applicable SRSS performance class after fusion using two SRS

	SRS 1 performance class					
SRS 2 performance class	**A**	**B**	**C**	**D**	**E**	**F**
A	B	B	C	D	E	F
B	B	C	C	D	E	F
C	C	C	D	D	E	F
D	D	D	D	E	E	F
E	E	E	E	E	F	F
F	F	F	F	F	F	F

The limitations in accordance with Table 6 are also valid for a combination of more than two SRS.

Table 6 is limited to one time use (consecutive combinations are not considered).

NOTE A combination of a first SRS claiming performance class A with a second claiming A and a third claiming B would be limited to B after fusion.

Verification by analysis shall be done.

6.2.8 Response time after fusion

The time from a change of a measured physical property until the corresponding change of the safety related information provided at the output unit of an SRSS using fusion of two or more SRS shall be specified by the SRSS integrator.

6.2.9 Verification and validation after fusion

The SRSS integrator shall verify and/or validate the SRSS in accordance with 6.2.3, 6.2.4 and 6.2.7.

This might require measures for further calibration.

EXAMPLE When SRS are combined in an SRSS, the following calibration issues may arise:

- providing measurement in relative or absolute data;
- providing measurement in different physical units;
- spatial transformation;
- projection (e.g. project 3D data into 2D space);
- different coordinate systems (e.g. Euclid, polar, cylindrical);
- different metric units and scaling.

6.3 Calibration at user side

6.3.1 General

The manufacturer of an SRS/SRSS shall define if a calibration procedure is required in the application to achieve the stated detection capability and fulfil the requirements of 5.8.

EXAMPLE Calibration procedure could be required if:

- measurement accuracy of the SRS/SRSS will change over time and, following the detection, capability is beyond the limits as defined by the manufacturer, which could result in a failure to danger or loss of normal operation;

- correction of failures of measurement accuracy are required by using adjustment of the SRS/SRSS in the application to achieve the detection capability during set into operation (e.g. by determination of temperature in the application as basis for adjustment used for reduction of "systematical errors").

If the SRS/SRSS provides an auto-calibration and adjustment function during operation, the SRS/SRSS shall not fail to danger if the calibration acceptance criteria are not achieved.

6.3.2 Calibration procedure and equipment

The manufacturer shall:

– describe the procedure of calibration by the user:
  - define when and how the calibration procedure shall be performed;
  - state which equipment is needed for the calibration procedure; or

– provide the necessary equipment:
  - describe installation, configuration and operation mode of required equipment and/or SRS/SRSS as setup;
  - define measures for verification and/or validation.

NOTE The calibration procedure could be executed after a SRS/SRSS has been installed before operation starts or after re-installation or exchange of components of a SRS/SRSS or a periodical re-calibration.

When one or more software program(s) is involved in the calibration procedure, for example for acquisition, processing, recording calculation or analysis of calibration data, it shall be developed in accordance with the standard for the SCS. Measures shall be appropriate for demand rate and impact of the calibration procedure performed in an SRS/SRSS of a defined performance class.

6.3.3 Verification and validation of calibration

The manufacturer shall define

– conditions (e.g. mounting position, environmental) during verification/validation,

– acceptance criteria for verification/validation to start or exit a calibration procedure (e.g. measurement uncertainty; time of operation),

– adjustment of the SRS/SRSS if the accuracy is outside the calibration acceptance criteria,

– inaccuracies of calibration procedure and their consideration in acceptance criteria, and

– conditions during calibration procedure.

The supplier shall provide information about how the results of the calibration procedure shall be documented at user side. The SRS/SRSS shall not fail to danger if the calibration acceptance criteria are not achieved.

EXAMPLE Acceptance criteria are:

- for a relative humidity (RH) sensor, the calibration acceptance criteria is for example ± 2 %;
- for distance measurement, it could be a limit in measurement accuracy and measurement uncertainty.

NOTE 1 Verification and adjustment can be executed more than one time to achieve required acceptance criteria.

NOTE 2 Verification can be executed by field tests in accordance with 8.5.

7 Operation, maintenance and modification phases

The manufacturer of an SRS/SRSS shall define appropriate measures to

– achieve safety related functions during operation,

– verify safety related functions during maintenance, and

- achieve safety related function in case of modification.

The supplier of an SRS/SRSS shall give appropriate information for operation, maintenance and installation within the information for use.

8 Verification and validation

8.1 General

Verification and validation shall be carried out for ensuring systematic capabilities of an SRS/SRSS.

8.2 Verification of an SRS/SRSS

The requirements given in the safety requirement specification of the SRS/SRSS shall be verified by analysis and/or testing during design and development.

The manufacturer of an SRS/SRSS with a performance class D, E, and F shall establish a verification plan as a document that includes

- references to specific requirements of the safety requirement specification for SRS/SRSS,
- details of when the verification take place during design and development,
- details of the persons, departments or units who carry out the verification,
- the selection of verification by analysis in accordance with 8.4,
- the selection of verification by testing in accordance with 8.5 by reference to the test plan and resulting document, and
- acceptance criteria and means to be used for the evaluation of verification results.

NOTE 1 The verification plan of an SRS/SRSS can be part of the overall verification and validation plan of the SCS.

NOTE 2 The verification plan can be part of a safety plan of an E/E/PES.

The reference to specific requirements of the safety requirement specification for SRS/SRSS can be achieved by a requirements management tool which shall be referenced inside the verification plan if applicable.

Table 7 shall be applied unless the standard being used for the functional safety of the SCS has different requirements.

Table 7 – Means to be used for evaluation of verification measures and verification results

	SRS/SRSS performance class					
Means/ verification measure	**A**	**B**	**C**	**D**	**E**	**F**
Review of verification plan and results	Not required	Not required	Not required	Check for: - completeness - proper implementation	Check for: - completeness - proper implementation	Check for: - completeness - proper implementation
Review of fulfillment of safety requirement specification	Check for: -fulfillment	Check for: -fulfillment	Check for: -completeness of requirements; -proper implementation; -fulfillment	Check for: -completeness of requirements; -proper implementation; -fulfillment.	Check for: -completeness of requirements; -proper implementation; -fulfillment.	Check for: -completeness of requirements; -proper implementation; -fulfillment.
Review of analysis	Not required	Not required	Check for: -proper method -proper implementation -no failure to danger condition	Check for: -proper method -proper implementation -no failure to danger condition	Check for: -proper method -proper implementation -no failure to danger condition	Check for: -proper method -proper implementation -no failure to danger condition
Review of tests	Check for: - proper test plan - tests fulfilled	Check for: - proper test plan - tests fulfilled	Check for: - proper test plan - tests fulfilled	Check for: - proper test plan - tests fulfilled	Check for: - proper test plan - tests fulfilled	Check for: - proper test plan - tests fulfilled
Review of information for use	Not required	Not required	Not required	Check for: -completeness in accordance with Clause 8	Check for: -completeness in accordance with Clause 8	Check for: -completeness in accordance with Clause 8

Corrective actions as result of reviews shall be defined and set in place if Table 7 is not fulfilled.

Corrective actions shall be implemented and verified again in accordance with Table 7.

8.3 Validation of an SRS/SRSS

The manufacturer of an SRS/SRSS shall define measures for validation over the life cycle considering:

- correct integration of an SRS/SRSS (e.g. mounting or safety related information provided by the output unit);
- appropriate risk reduction as intended by the safety related functions;
- absence of intolerable hazards produced by the SRS/SRSS (e.g. optical radiation in accordance with 4.2.2.2);
- appropriate test method and test set up in accordance with 8.5.3 and 8.5.4 (e.g. for field test or endurance test);
- appropriate analysis methods in accordance with 8.4 (e.g. inspection);
- procedures for test and analysis;
- documentation of test and analysis result.

Validation measures and procedures shall be documented by the manufacturer and provided by the supplier in an appropriate way within the information for use.

If validation measures and procedures result in non-conformity, appropriate measures at user side shall be provided by the supplier within the information for use.

NOTE 1 This can contain the need for information of the supplier on non-conformity items.

The user shall be informed about the need for documentation and review of validation results if applicable.

Definition of validation measures and procedures are usually only feasible in a late stage of design and development. Results of SRS/SRSS verification shall be considered and first inspections/tests in the application can be necessary. Because of these considerations, this document does not require a validation plan comparable to a verification plan.

NOTE 2 The documentation is separated into portions defined by the manufacturer and the supplier. The manufacturer documentation addresses measures and processes related to his domain expertise. The supplier is assumed to be more familiar with the application at the user side and the available competence.

8.4 Analysis

Analysis shall be used for verification and validation of the

- impact of component(s) behaviour on the detection capability of an SRS/SRSS,
- conformity of an SRS/SRSS with the safety requirement specification and this document (e.g. SRS/SRSS function as defined in 5.2),
- correct integration at the user interface of a
  - SRS into an SRSS if applicable,
  - SRS/SRSS into a SCS if applicable, and
  - SRS/SRSS into a machine if applicable, and
- performance of the SRS/SRSS at the end user application as defined by the manufacturer of an SRS, SRSS, SCS and/or machine.

A quantitative analysis shall be performed with regard to prevention of failure to danger conditions on SRS/SRSS of performance class C, D, E and F.

Safety analysis used for verification is performed at the appropriate level of abstraction during design and development of an SRS/SRSS.

Quantitative analysis methods predict the frequency or duration of failures while qualitative analysis methods identify failures but do not predict the frequency or duration of failures.

Both types of analysis methods depend upon knowledge of the relevant fault types and fault models.

Qualitative analysis methods include but are not limited to

- qualitative FMEA at system, design or process level,
- qualitative FTA,
- estimation by simulation models,
- analysis by inspection, and
- analysis by formal design review.

NOTE 1 Inspection during verification of an SRS/SRSS is a method requesting domain expertise in sensing technology and dependability of detection capability.

Quantitative safety analysis complements qualitative safety analysis. They are used to verify against target values as defined in Table 4, Table 5, Formula (1) and Formula (G.1).

Quantitative analysis methods include but are not limited to:

- quantitative FMEA;
- quantitative FTA;
- prediction by simulation models like:
  - Markov models;
  - reliability block diagrams respective reliability models.

NOTE 2 Another criteria for the choice of appropriate analysis methods is the way they are conducted. Inductive analysis methods (e.g. FMEA, Markov modelling) are bottom-up methods that start from a known cause and forecast unknown effects. Deductive analysis methods (e.g. FTA and reliability block diagram) are top down methods that start known effects and seek unknown causes.

8.5 Test

8.5.1 General

Tests shall be used for verification respective validation of the:

- impact of component(s) behaviour on the detection capability of an SRS/SRSS;
- correctness of model(s) used for simulation if applicable;
- conformity of an SRS/SRSS with the safety requirement specification and this document, (e.g. SRS/SRSS function as defined in 5.2);
- correct integration at the user interface of an:
  - SRS into an SRSS if applicable;
  - SRS/SRSS into a SCS if applicable;
  - SRS/SRSS into a machine if applicable;
- performance of the SRS/SRSS at the end user side as defined by the manufacturer of an SRS, SRSS, SCS and/or machine.

The supplier shall describe test and test set up for verification respective validation to be performed at user side within information for use.

NOTE SCS and/or machine are stated to cover potential additional information generated during integration of an SRS/SRSS which are relevant for the final performance of the SRS/SRSS at end user side. No further requirements will be given for SCS and/or machine supplier.

8.5.2 Test classification

Tests shall be defined by the manufacturer using one or more of following:

- type test (e.g. used for type test examination of detection capability during design and development of an SRS);
- qualification test (e.g. used to qualify a shipment of components used in an SRS);
- routine test (e.g. used to test 100 % of an component in a production line);
- endurance test (e.g. used to show durability of an item over an assumed lifetime);
- laboratory test (e.g. used to verify correctness of models used as part of simulation during design and development);
- maintenance test (e.g. used to verify correct localization of SRSS safety related zone at operator side after modification on machines);
- system test (e.g. used for verification of correct integration of an SRS into an SRSS);
- simulation test (e.g. used for verification of safety related functions of an SRS under environmental conditions as defined inside the SRS representative for the intended use);

- acceptance test (e.g. agreed between an SRS manufacturer and SCS integrator used to get acceptance on defined requirements);
- field test (e.g. used for verification of safety related functions und real environmental conditions at the operator side).

NOTE 1 The type tests could be performed by the manufacturer or an authorized company, on one or more devices under test taken from the normal production or pre-production, and are intended to assess the performances strictly dependent on the design of the SRS/SRSS. They are performed on new developed products or on products on which significant design modifications have been made.

NOTE 2 The acceptance tests could also be performed by the manufacturer, usually in the presence of the customer which can be the integrator, in order to verify if the SRS supplied by the manufacturer meet the requirements outlined in the specification.

NOTE 3 After installation and during operation of the SRS/SRSS, it could be necessary to verify the integrity of detection and/ or localization of the safety related zone with a defined maintenance test at operator side. In this case, the manufacturer informs the operator on the necessary procedure and on the necessary equipment. Maintenance tests are often related to country specific and application specific regulations, which can define for example cycle of test when maintenance test has to be performed.

NOTE 4 System test could be impacted if a safety related function of an SRS/SRSS is performed as a function block by software module which can be tested. Tested software modules could be further verified during a software integration test as system test using for example the SCS where it is executed.

NOTE 5 During field test on operator side, it could be beneficial to define in advance within the test plan which influences on the SRS/SRSS safety related function are of major interest and to record them in an appropriate way. For example, fog could be recorded by a timestamped camera that observes the same zone as the SRS/SRSS during the field test.

8.5.3 Test method and test setup

The manufacturer of an SRS/SRSS shall define the test methods.

NOTE 1 An example of a test method is a light interference test for normal operation and no failure to danger by using a tungsten halogen source of defined behaviour as representation for natural light during a laboratory test.

If a laboratory test is applied, test methods should comply as far as reasonable with the metrological principles concerning validation, measurement traceability and estimation of measurement uncertainty. Requirements related to testing equipment should comply as far as reasonably practicable with the provisions concerning accuracy and calibration.

NOTE 2 Guidance about good practices can be found in ISO/IEC 17025.

NOTE 3 Other documents could be applicable (e.g. ISO/IEC Guide 98-3).

The test setup shall be defined by the manufacturer of an SRS/SRSS and shall take the following into account as far as reasonably practical:

- mounting conditions and mounting brackets as defined by the manufacturer;
- size of sensing zone(s) as defined by the manufacturer;
- the use of output information of:
  - sensing unit;
  - processing unit;
  - output unit,
- reproducible representations of safety related object properties;
- reproducibility of test setup and used test equipment.

NOTE 4 The choice of the test setup and the way to provide a physical property of a safety related object in an accurate and traceable way as the input information of the SRS/SRSS device under test (DUT) is an issue from the technical and economic point of view. For example, extensive equipment could be needed in which all factors influencing the result and reproducibility of the test are sufficiently controlled. The equipment used in the laboratory test setup could be, for certain tests (for example snow test chamber, fog producing chamber) inappropriately expensive. Therefore, in example, an analysis could be used to identify if and which kind of test equipment is appropriate for the intended sensor performance class and the specified performance (for example high versus low limits on fog). In one case, investment in laboratory test equipment seems to be reasonable for a sensor performance class E but inappropriate for performance class A. Analysis could result in an alternative approach using field test instead of laboratory test for type testing.

Test setup contains the SRS/SRSS representing device under test and the equipment used to perform the test. Test methods and test setup on environmental testing shall be done as far as reasonably practical and applicable in accordance with appropriate standards (e.g. IEC 60068 (all parts), IEC 61496 (all parts), IEC 60529, IEC 60947-5-2).

Test methods and test setup on EMC for functional safety shall be done if applicable in accordance with IEC 61000-6-7:2014 as defined for the appropriate SIL unless a relevant application or product specific standard is applied (e.g. IEC 60947-5-3, IEC 61496-1 or IEC 62061).

NOTE 5 If the test setup for type test is not available in standards such as those of the IEC 60068 series, alternatives can be useful. One example is given in [2]. Another example are test setup(s) as defined in product standards for safety related sensors like IEC 61496 (all parts).

8.5.4 Test piece

The manufacturer of an SRS/SRSS shall define test pieces if they are used for:

- test of the detection capability;
- test of proper location of safety related zone(s);
- test for appropriate safety related information during the test piece intrusion.

The characteristic of the test piece shall be defined taking into account:

- sensing technology/technologies used in an SRS/SRSS;
- presentation of relevant object properties as defined in 5.8.2 used for the detection;
- test classification(s) using the test piece (e.g. type test, routine test, maintenance test); and
- intended application of the SRS/SRSS.

As far as reasonably practical, test pieces shall be used as defined in appropriate standards.

The manufacturer of an SRS/SRSS shall specify test pieces and the supplier shall document their properties in the information for use if they are used for validation of SRS/SRSS detection capability.

NOTE Test piece is only a part of the overall test equipment. It is of special interest because of use in application by end user to perform a maintenance test or during type test at manufacturer side.

EXAMPLE Definitions are:

- test pieces representing adult persons for AOPD type testing using optical sensing technology in IEC 61496-2; and
- test pieces representing children in application standard EN 16580 or in IEC 61032.

8.5.5 Test plan and test results

The manufacturer of an SRS/SRSS shall define and document a test plan covering:

- items on verification and validation by test as listed in 8.5.1;
- items on test classification as listed in 8.5.2;
- items on test methods and test setup as listed in 8.5.3;
- test procedure (including criteria for fail or passing a test);
- number of devices under test (e.g. components, SRS, SRSS); and
- unambiguous identification information of devices under test (e.g. serial number).

– measures as classified in Table 6.

NOTE On some test methods such as acceptance tests, it could be beneficial to define in example a common test plan between manufacturer of an SRS and customer (e.g. integrator of an SRS into SCS). This could reduce the risk that undefined test setup and equipment would lead to different results.

Test results shall be documented in test report(s). Test results shall be marked as "failed" or "passed".

Other wording can be used but should be unique and easy to identify the result of the test by a person which is not in charge of the test (e.g. integrator doing review of test results of an acceptance test).

Test results shall be used for:

– review to show compliance with test plan; and

– verification of safety requirement specification.

9 Information for use

The information for use of the SRS/SRSS shall provide relevant information for installation, use and maintenance. This shall include a comprehensive description of the equipment and mounting.

NOTE 1 Information for use is documented within the customer documentation. If the information for use is titled "Safety Manual", it can be confused with specific requirements within IEC 61508 (all parts).

The information shall be appropriate for the user(s) of an SRS/SRSS as defined by the supplier and shall take the following into account:

– field of application;

– limits of use (especially need for validation if SRS/SRSS is applicable to specific application at end user side);

– integration of two or more SRS into an SRSS;

– integration of one or more SRS/SRSS into an SCS.

The required information for use (where relevant) includes, but is not limited to, that given in Table 8.

NOTE 2 Roles defined as being part of a supply chain considered as addressed group of information for use are shown in Annex B.

Table 8 – Overview of information for use to be provided

Clause/ subclause	Overview of information for use to be provided (see reference for full text)
4.3	The SRS/SRSS performance class and the level of safety performance (PL, SIL or SIL$_{cl}$) and the referenced standard
5.2	The SRSS function in accordance with general description of Table 2.
5.5	Information on the sensing zone(s) if applicable.
5.6	Information on safety related zone(s).
5.7	Information on automation related zones if applicable.
5.8.2.1 5.8.2.2 5.8.2.3	Limits of the physical properties (e.g. properties used for person detection like length, area, volume, reflectivity, velocity and/or properties used for hazardous object detection) within which the SRS/SRSS function is performed.

Clause/ subclause	Overview of information for use to be provided (see reference for full text)
5.8.3.1 5.8.3.3 5.8.3.4	The environmental influences relevant for the dependability (failure to danger and normal operation) of the detection capability of the SRSS.
5.8.3.3	Relevant information on the results of analysis of the influence of relevant environmental conditions on the loss of detection capability and consequences if the limits are not achieved in the application.
5.8.3.3	Information if one of the additional approaches of Annex G are used.
5.9.2	Information on mounting of a sensing unit/SRS/SRSS.
5.9.3	Safety related information (measurement information, decision information and confidence information if applicable) provided by the output unit.
5.9.3.1	The signal to initiate the fault reaction function and its fault response time if applicable.
5.9.3.3	The response time.
6.1	The Information for integration and installation.
6.2.1	Information for use of each fused SRS.
6.2.2 6.2.3 6.2.4 6.2.5 6.2.6 6.2.7	The limits of use after fusion (detection capability, sensing zone(s), environmental conditions in type and limits for no failure to danger and for normal operation, safety related information, SRSS performance class) of the SRSS.
6.2.8	The response time after fusion into an SRSS.
6.3.1 6.3.2	If applicable, calibration procedure in the application to achieve the stated detection capability.
6.3.3	Information of verification and validation of calibration at user side.
7	Information for operation, maintenance and modification.
8.5.1	Description of test and test set up for verification respective validation to be performed at user side use.

Annex A
(informative)

Examination of systematic capabilities

The examination of systematic capabilities is required by functional safety standards for safety related control systems used for the protection of persons. Different approaches by using safety related sensor standards are possible (see Figure A.1 as an example). The list of used standards should be stated and included in the information for use of a SRS/SRSS.

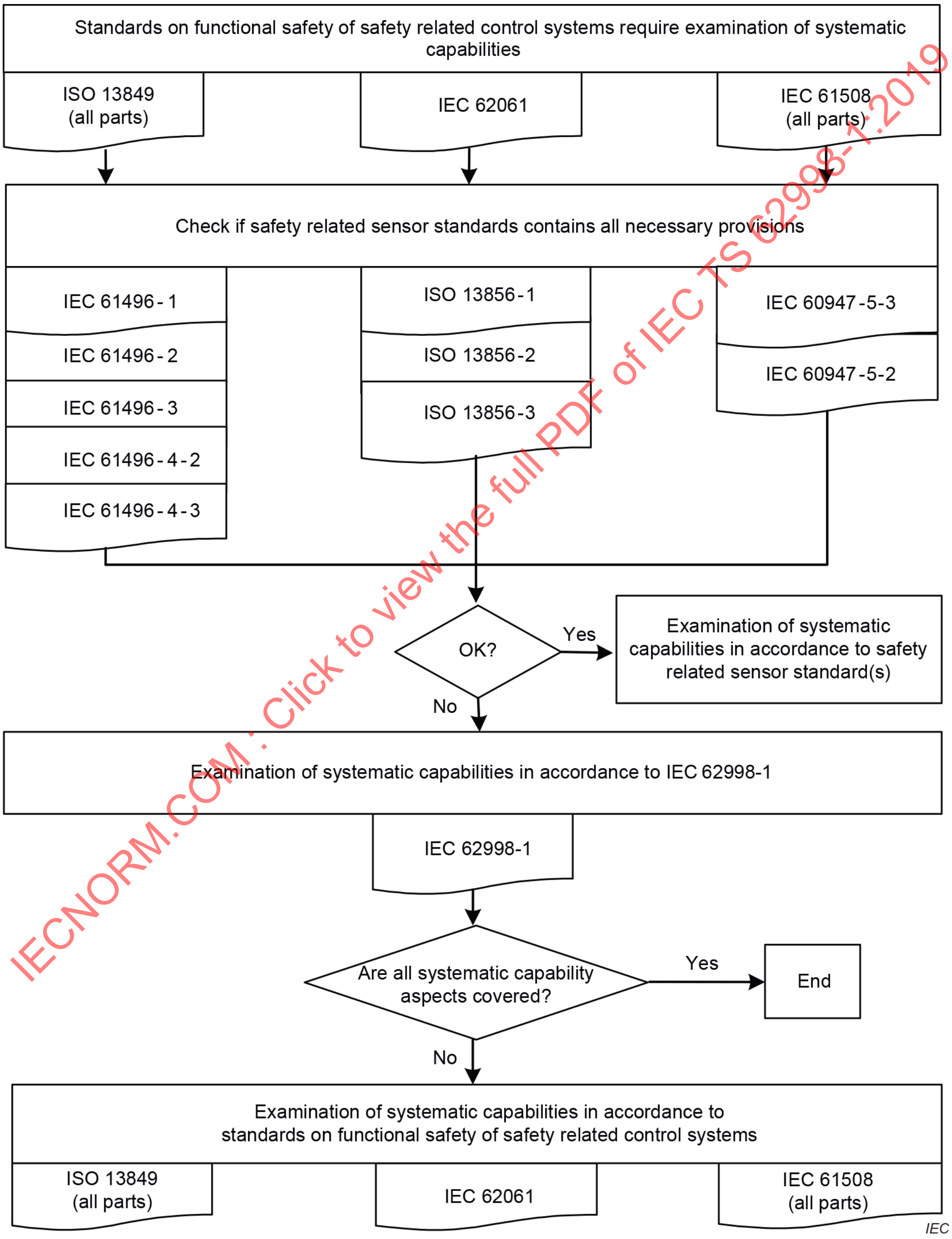

Standards on functional safety of safety related control systems require examination of systematic capabilities
ISO 13849 (all parts)
IEC 62061
IEC 61508 (all parts)
Check if safety related sensor standards contains all necessary provisions
IEC 61496-1
IEC 61496-2
IEC 61496-3
IEC 61496-4-2
IEC 61496-4-3
ISO 13856-1
ISO 13856-2
ISO 13856-3
IEC 60947-5-3
IEC 60947-5-2
OK?
Yes
Examination of systematic capabilities in accordance to safety related sensor standard(s)
No
Examination of systematic capabilities in accordance to IEC 62998-1
IEC 62998-1
Are all systematic capability aspects covered?
Yes
End
No
Examination of systematic capabilities in accordance to standards on functional safety of safety related control systems
ISO 13849 (all parts)
IEC 62061
IEC 61508 (all parts)
IEC

Figure A.1 – Example for examination of systematic capabilities using safety related sensor standards

It is an additional possibility to examine systematic capability by combination of those aspects covered by the safety related sensor standard and any not covered by using this document.

Annex B
(informative)

User groups

B.1 User groups of SRS/SRSS and groups addressed by this document

This document addresses different user groups with the content and following to that user groups using SRS/SRSS as a product. Table B.1 gives an overview.

Table B.1 – Roles and task of addressed user groups

	SRS/SRSS manufacturer	SRS Integrator into SRSS	SRS/SRSS integrator into SCS	Machinery manufacturer	End user side
Content of this document	Using content as: - manufacturer of an SRS, and - supplier of an SRS into an SRSS or SCS.	Using content as: – integrator of an SRS into an SRSS; and -supplier of an SRSS into an SCS.	Not addressed	Not addressed	Not addressed
SRS as product	Responsible as Manufacturer and supplier of an SRS - performing routine test and/or type test	- User of the SRS as integrator into SRSS -to be instructed by information for use of SRS	- User of the SRS as integrator into SCS -to be instructed by information for use of SRS	-User of an SRS as manufacturer and supplier of machinery -to be instructed by information for use of SRS	-User of an SRS safety related function - performing maintenance tests -performing field tests -to be instructed by information for use of SRS
SRSS as product	Responsible as Manufacturer and supplier of an SRSS - for example performing routine test and/or type test	Responsible as integrator and supplier of an SRSS -for example performing system test of an SRSS as routine test and/or type test	Responsible as integrator of an SRSS into SCS -for example performing system test of SCS as routine test and/or type test	User of an SRSS as manufacturer and supplier of machinery - to be instructed by information for use of SRSS	User of an SRSS safety related function -performing maintenance tests -performing field tests -to be instructed by information for use of SRSS

NOTE 1 The table shows in first row the addressed group. An organization could cover different groups. For example, the sensor manufacturer can be an integrator, the machine manufacturer can be an integrator, or the manufacturer of a programmable logic control can be an integrator.

NOTE 2 The table shows in first column the fields of interests from addressed group point of view.

NOTE 3 The other cells of the table show roles and examples of task an addressed group takes.

B.2 User groups addressed by fusion

The pure definition of fusion (see 3.5.3) lead to the result that each step of integration, starting from sensing unit up to the complete machine, their interconnection in a plant and corresponding execution of logic functions, is an act of fusion.

This document limits the term "fusion" actual to integration of two or more SRS into an SRSS addressing a specific user group (see No. 5 of Table B.2). Table B.2 shows different integration types and corresponding user groups addressed by this document based on differentiation by used elements, performed functions and further justifications.

Table B.2 – Addressed user groups for different integration types using sensing unit, SRS/ SRSS as element or SRS as subsystem

No.	Integration type	User group addressed by this document	Covered lement/ subsystem in this document	Performed function after integration	Justification
1	One or more sensing units into SRS	SRS manufacturer	Sensing unit, processing unit, Input/output unit deliver safety related information	SRS function in accordance with Table 2	Fits into scope of this document Complexity of the content of this document requires high competence in use of one sensing technology
2	One or more Sensing unit(s) directly into SRSS or combination of an sensing unit with an SRS into SRSS	Not addressed	-	-	The combination of sensing functions provided by sensing units requires deep knowledge of the sensing technology. Processing inside the SRS is seen as necessary before further integration into an SRSS is considered.
3	One or more Sensing unit (s) into SCS	Not addressed	-	-	Large difference in required competences between overall safety function and sensing unit delivering safety related information. Not considered and not covered in this document.
4	One SRS into one SRSS	Not addressed	-	-	No practical use foreseen. Is still one SRS. Addressed by SRS manufacturer group (see No.1).
5	Two or more SRS into SRSS	SRS integrator into SRSS	Processing unit Input/output unit deliver safety related information Logic functions based on safety related information SRS as subsystem performing SRS function in accordance with Table 2	SRSS function in accordance with Table 2 with execution of logic functions inside SRSS (see. Figure C.2)	Fit into scope of this document; 6.2 applies Complexity of the content of this document SRS fusion into SRSS can be accomplished with limited competence in use of sensor technologies

No.	Integration type	User group addressed by this document	Covered lement/ subsystem in this document	Performed function after integration	Justification
6	Two or more SRS into SRSS	SRSS manufacturer	Sensing unit Processing unit Input/output unit deliver safety related information Logic functions based on safety related information SRS as subsystem performing SRS function in accordance with Table 2	SRSS function in accordance with Table 2 with execution of logic functions inside SRSS (see. Figure C.2)	Fit into scope of this document Complexity of the content of this document requires high competence in use of different sensor technologies
7	Two or more SRSS into SRSS	Not addressed	-	-	No practical use foreseen. For this integration type, the necessary SRS shall be combined directly into final SRSS (addressed by SRS integrator into SRSS) or the integration type might be addressed by full approach as SRSS manufacturer.
8	One or more SRS in combination with one or more SRSS into SRSS	Not addressed	-	-	It is assumed that the risk would be too high for missing relevant influences at this type of combination. For this integration type, the necessary SRS shall be combined directly into final SRSS (addressed by SRS integrator into SRSS) or the integration type might be addressed by full approach as SRSS manufacturer.

Annex C
(informative)

Functional decomposition and/or integration

SRS/SRSS function in accordance with 5.2 content safety related function(s) and optional automation related function(s). The safety related function(s) is based on physical properties of person, parts of person and/or hazardous object(s) as shown in Figure C.1

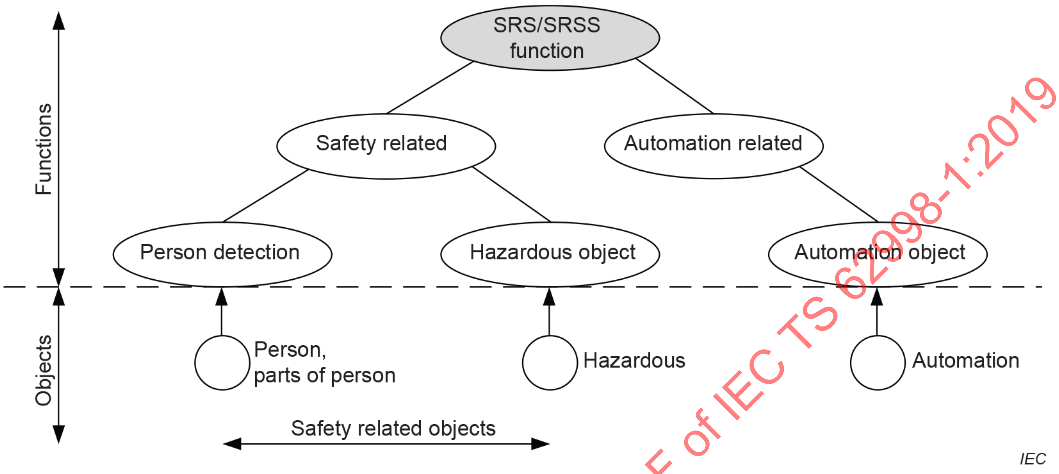


Figure C.1 – Interconnection of functions and objects

The safety related function(s) of an SRS/SRSS might be used to perform a safety function in an SCS (subfunction as a subsystem in accordance with e.g. IEC 62061). Figure C.2 shows an example in accordance with architecture of Figure 4 performing safety related function and their integration into an SRSS.

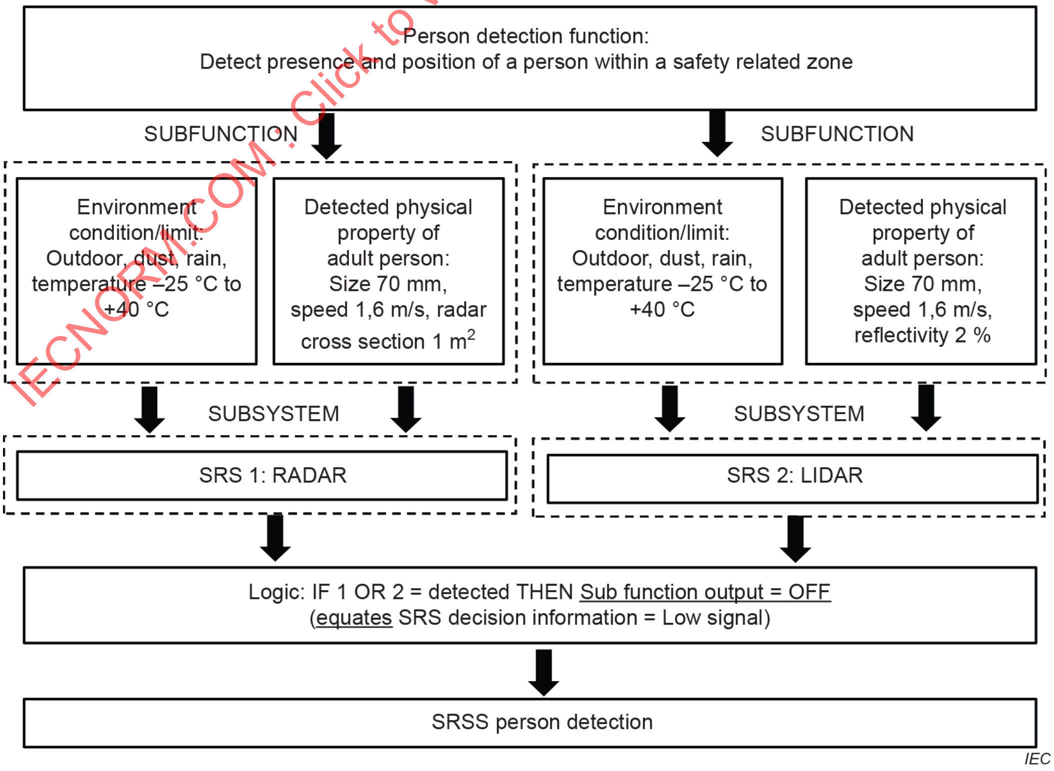

Person detection function:
Detect presence and position of a person within a safety related zone
SUBFUNCTION
SUBFUNCTION
Environment condition/limit: Outdoor, dust, rain, temperature –25 °C to +40 °C
Detected physical property of adult person: Size 70 mm, speed 1,6 m/s, radar cross section 1 m²
Environment condition/limit: Outdoor, dust, rain, temperature –25 °C to +40 °C
Detected physical property of adult person: Size 70 mm, speed 1,6 m/s, reflectivity 2 %
SUBSYSTEM
SUBSYSTEM
SRS 1: RADAR
SRS 2: LIDAR
Logic: IF 1 OR 2 = detected THEN Sub function output = OFF
(equates SRS decision information = Low signal)
SRSS person detection
IEC

Figure C.2 – Example of functions performed in an SRSS

Annex D
(normative)

Generation and application of simulation models

D.1 General

Annex D provides information for the generation and application of simulation models used for:

- design analysis which contains a simulation in accordance with 5.4; or
- verification of limits of use instead or in addition to physical test set up as described in 8.5.

D.2 Recommendations for use

The manufacturer shall determine the complexity of the SRS/SRSS.

A SRS/SRSS is defined as being of low complexity if:

- the behaviour under systematic condition can be completely determined; and
- a deenergize to trip principle is used.

In case of low complexity, Table D.1 does apply and in all other cases Table D.2 for high complexity does apply.

D.3 Simulation objectives and measures to achieve them

If the use of simulations is mandatory according to 5.4, the appropriate measures and objectives (with the goal to detect and prevent safety-relevant failures) shall be taken from Table D.1 for low complexity and from Table D.2 for high complexity.

Table D.1 – Simulation objectives and measures for SRS/SRSS of low complexity

Measure/objective for sensor performance class	D	E	F
Use of simulations to …			
… support design and development	Recommended	Recommended	Highly recommended
…perform an impact analysis of influences and failures	Recommended	Highly recommended	Highly recommended
…validate the SRS/SRSS performance	Recommended	Highly recommended	Highly recommended
Impact analysis of prerequisites, limitations and approximations on simulation results	Highly recommended	Highly recommended	Highly recommended
Impact analysis of numerical precision and tolerances on simulation results	Recommended	Recommended	Highly recommended
Decomposition and separate verification of simulation sub-parts	Recommended	Recommended	Recommended
Use of computer-aided design tools that have an extensive history of satisfactory use	Recommended	Recommended	Recommended
Development of the simulation model according to the requirements of IEC 62061:2005, 6.11.3.1 and 6.11.3.4	-	-	Recommended
Quantitative comparison of reference test results with simulation output including boundary data and sensitivity analysis	-	Recommended	Highly recommended
Qualitative comparison of reference test results with simulation output (trends, general behaviour)	Recommended	-	-
Modelling on a component level including boundary data	-	-	Recommended
Modelling at a module level including boundary data of peripheral units	Recommended	Recommended	-
Modelling by combination of verified models of subparts and known interaction behaviour.	Recommended	Recommended	Recommended

Key

-: There is no recommendation for or against the use of simulations in design/development and validation of the SRS/SRSS

Recommended: The use of simulation in design/development and validation is recommended for this sensor performance class. If the effort to develop a simulation model to analyse the systematic behaviour of the SRS/SRSS would be inappropriate and tests can alternatively provide sufficient knowledge on the systematic capabilities, simulations can be omitted.

Highly recommended: The use of simulation in design/development and validation is highly recommended for this sensor performance class. If simulations are not used, then the rationale behind not using it shall be detailed.

Table D.2 – Simulation objectives and measures for SRS/SRSS of high complexity

Measure/objective for sensor performance class	D	E	F
Use of simulations to …			
… support design and development	Recommended	Highly recommended	Highly recommended
…perform an impact analysis of influences and failures	Highly recommended	Highly recommended	Highly recommended
…validate the SRS/SRSS performance	Highly recommended	Highly recommended	Highly recommended
Impact analysis of prerequisites, limitations and approximations on simulation results	Highly recommended	Highly recommended	Highly recommended
Impact analysis of numerical precision and tolerances on simulation results	Recommended	Highly recommended	Highly recommended
Decomposition and separate verification of simulation sub-parts	Recommended	Recommended	Recommended
Use of computer-aided design tools that have an extensive history of satisfactory use	Recommended	Recommended	Recommended
Development of the simulation model according to the requirements of IEC 62061:2005, 6.11.3.1 and 6.11.3.4	-	Recommended	Recommended
Quantitative comparison of reference test results with simulation output including boundary data and sensitivity analysis	Recommended	Highly recommended	Highly recommended
Qualitative comparison of reference test results with simulation output (trends, general behaviour)	-	-	-
Modelling on a component level including boundary data	-	Recommended	Recommended
Modelling at a module level including boundary data of peripheral units	Recommended	-	-
Modelling by combination of verified models of subparts and known interaction behaviour.	Recommended	Recommended	Recommended

<table>
<tr><th>Measure/objective for sensor performance class</th><th>D</th><th>E</th><th>F</th></tr>
<tr><td colspan="4"><b>Key</b>
-: there is no recommendation for or against the use of simulations in design/development and validation of the SRS/SRSS
"Recommended": The use of simulation in design/development and validation is recommended for this sensor performance class. If the effort to develop a simulation model to analyse the systematic behaviour of the SRS/SRSS would be inappropriate and tests can alternatively provide sufficient knowledge on the systematic capabilities, simulations can be omitted.
"Highly recommended": The use of simulation in design/development and validation is highly recommended for this sensor performance class. If simulations are not used, then the rationale behind not using it shall be detailed.</td></tr>
</table>

D.4 Verification

Simulations used for design or validation shall be verified (see Figure D.1).

The verification approach shall be able to detect at least the following causes for errors and inaccuracies:

- wrong or inaccurate input data;
- wrong or inaccurate simulation model;
- wrong or inaccurate simulation tools.

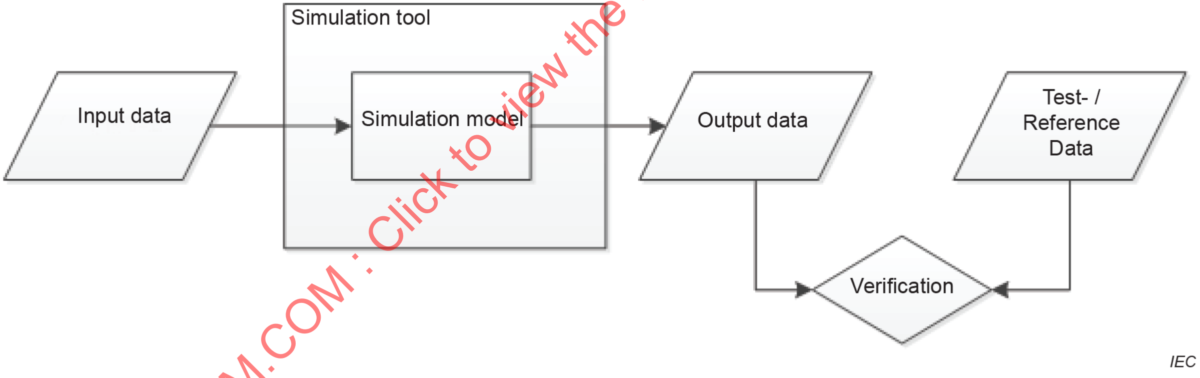


Figure D.1 – Verification process

Simulations shall be verified by a detailed comparison between the simulation results and the experimental/test results of a dedicated reference test.

The reference situation used as ground truth shall:

- comprise all system parts that are addressed by the simulation model;
- allow for a quantitative comparison if the simulation is used to model quantitative behaviour;
- represent a situation that has relevance for the safety function (e.g. critical failure case or limit scenario).

The comparison shall check for agreement with respect to:

- qualitative and quantitative behaviour;
- predicted accuracy;

- sensitivity of critical parameters.

Additional measures to verify the simulation model can be:

- walk-through review of the simulation model and model input data;
- comparison of input data from different sources;
- specific test and verification of sub-modules;
- check if statistical distributions derived from measurement data can be reproduced by stochastic simulations (e.g. Monte-Carlo simulations);
- comparison of simulation results with results generated by other simulation models.

Additional means to validate simulation tools can be (see IEC 62061:2005, 6.4.1.2 b):

- specific testing;
- independent validation of their output for the particular safety related system;
- documentation of tool configuration and related experience.

Annex E
(informative)

Child properties and behaviour

E.1 General

Children are defined in accordance with ISO/IEC Guide 50 as persons aged under 14 years.

Depending on age specific child development, the behaviour like moving strategies (e.g. crawling, walking, running) or exploration strategies (e.g. knowledge on potential risks, taking risk to learn) of children are different from adult persons.

The sizes representing the body or parts of body of a child are described in Clause E.2.

If test pieces are defined as representations of children or parts of children, see also 8.5.4. Test piece sizes are not necessarily equal with sizes of parts of a body as listed in Clause E.2. Specific application or limits in sensing technology might be a justification.

E.2 Sizes of parts of body

Tables E.1 to E.4 and Figures E.1 to E.4 show selected examples of children parts of body sizes. They are based on anthropometric data from Japan and USA. Out of these data, the minimum or maximum values for both sexes are used and the most limiting value listed as representative in the tables. As long as available, it is recommend to use the more recent data from Japan. If not available, data from USA might be used.

NOTE Further information is available in [3] and [4].

Table E.1– Body height children

Age years	5 % value mm		50 % value mm		95 % value mm	
	USA	**Japan**	**USA**	**Japan**	**USA**	**Japan**
1	686	712	725	779	785	849
2	796	812	841	874	904	918
3	869	890	932	960	994	1 029
4	928	960	994	1 015	1 065	1 098
5	989	1 020	1 070	1 076	1 150	1 164
6	1 044	1 081	1 136	1 158	1 205	1 231
7	1 104	1 134	1 198	1 206	1 271	1 274
8	1 144	1 198	1 246	1 286	1 335	1 351
9	1 210	1 130	1 299	1 299	1 399	1 421
10	1 249	1 289	1 347	1 376	1 453	1 519
11	1 318		1 408		1 511	
12	1 353		1 465		1 575	
13	1 400		1 522		1 643	

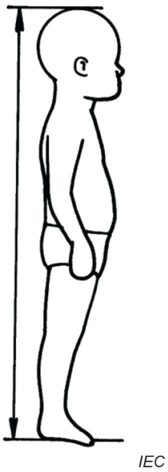


Figure E.1 – Body height children

Table E.2 – Chest depth children

Age years	5 % value mm		50 % value mm		95 % value mm	
	USA	**Japan**	**USA**	**Japan**	**USA**	**Japan**
1	89	96	110	113	118	128
2	98	105	116	113	126	128
3	103	110	119	121	135	131
4	108	112	123	124	138	137
5	110	112	128	126	147	139
6	116	113	133	131	151	144
7	121	122	137	135	156	148
8	118	129	138	137	164	153
9	126	122	144	145	171	153
10	125	133	146	151	175	172
11	134		157		197	
12	141		161		195	
13	153		171		221	

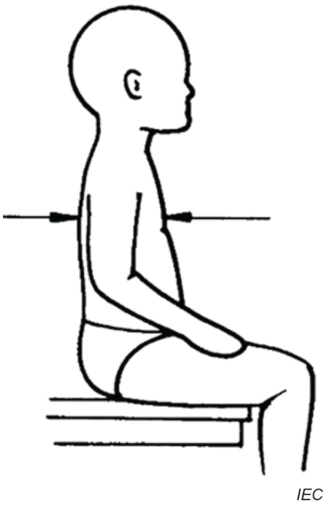


Figure E.2 – Chest depth children

Table E.3 – Head width children

Age years	**5 % value** mm		**50 % value** mm		**95 % value** mm	
	USA	**Japan**	**USA**	**Japan**	**USA**	**Japan**
1	115	125	124	133	131	146
2	124	126	131	136	140	147
3	126	131	133	140	141	152
4	128	132	136	142	144	153
5	129	134	137	144	146	154
6	131	136	138	145	147	156
7	131	136	140	144	149	155
8	133	138	140	148	149	158
9	134	138	142	146	150	157
10	134	135	142	149	151	160
11	136		143		152	
12	136		144		154	
13	137		145		153	

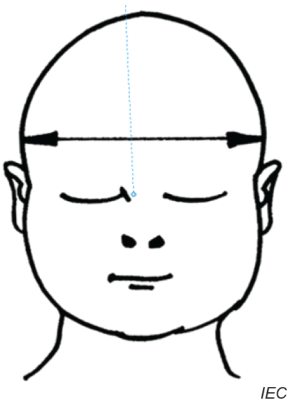
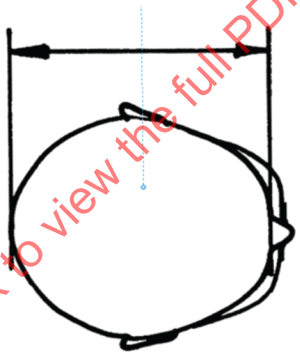


Figure E.3 – Head width children

Table E.4 – Head length children

Age years	5 % value mm		50 % value mm		95 % value mm	
	USA	**Japan**	**USA**	**Japan**	**USA**	**Japan**
1	149	146	161	156	168	171
2	160	153	172	162	184	174
3	165	155	175	165	185	178
4	167	158	178	168	189	178
5	169	157	179	168	192	178
6	173	162	182	172	194	183
7	171	161	181	172	193	181
8	170	164	183	172	195	181
9	172	161	185	176	197	185
10	173	164	185	176	196	186
11	174		186		198	
12	171		186		197	
13	173		189		198	



IEC

Figure E.4 – Head length children

Annex F
(informative)

Environmental influences

F.1 General

Annex F provides examples of how the list of environmental influences as described in 5.8.3.2 can be applied.

F.2 Example 1 for application of environmental influences

An SRS/SRSS based on an optical sensor is used to provide safety related sensor information for a collision prevention function of an autonomous (electrically driven) vehicle on an industrial site. The vehicle operates between manufacturing buildings and needs to cross unsheltered outdoor areas. The SRS/SRSS is located on the outside of the vehicle (unprotected from precipitation).

An analysis has identified the following relevant environmental influences for the SRS/SRSS:

- temperature and humidity;
- fog;
- precipitation (rain, hail, snow);
- solar radiation;
- condensation and icing;
- dust and sand;
- fauna;
- vibration and shocks;
- electrical and electromagnetic influences.

Not listed items out of the list of environmental influence in accordance with 5.8.3.2 are irrelevant in this particular example and have been omitted.

Relevant parts of the IEC 60721 (all parts) are IEC 60721-3-0 (Introduction) and IEC 60721-3-5 (Ground vehicle installations).

According to IEC 60721-3-5, the limits provided are extreme cases with a very low probability of being exceeded. Environmental influences reach the specified limiting values very rarely and only for a short time. For simplicity, storage conditions are neglected in this example.

Resulting environmental influences relevant for the detection according to environmental classification and application specific modifications are listed in the Table F.1.

Table F.1 – Example 1 of environmental influence and classes according to IEC 60721-3-5

Environmental influence	Class according to IEC 60721-3-5	Limits	Modification of limits	Remarks
Temperature	5K3	–40 °C to +40 °C		Low extreme occurs for approx. 10 h per year. High extreme occurs for approx. 5 h per year (see IEC 60721-2-1)
Change rate of temperature	5K3	5 K/min		Transition from indoor to outdoor or vice versa will possibly give rise to larger change rates
Relative humidity	5K3	95 %		
Rainfall	5K3	6 mm/min		Extreme rain occurs only for a few minutes per year
Snow	-	Shall be considered		No numerical limits specified in IEC 60721 (all parts)
Fog	-	Shall be considered		No numerical limits specified in IEC 60721 (all parts)
Icing		Shall be considered		No numerical limits specified in IEC 60721 (all parts)
Solar radiation		1 120 W/m^{2}	700 [W/m^{2}]	If hood can be used to shield direct solar radiation
Fauna	5B2	Insects shall be considered, mould growth		
Vibration (sinusoidal) amplitude/acceleration	5M2	3,3 mm at 2 Hz to 9 Hz 10 m/s^{2} at 9 Hz to 200 Hz 15 m/s^{2} at 200 Hz to 500 Hz		Operation in electrically driven vehicles on flat, smooth surfaces
Vibration (broadband) amplitude/acceleration	5M2	1 m^{2}/s^{3} at 10 Hz to 200 Hz 0,3 m^{2}/s^{3} at 200 Hz to 500 Hz		Operation in electrically driven vehicles on flat, smooth surfaces
Shock (peak acceleration)	5M2	100 m/s^{2}		Type I
Shock (peak acceleration)	5M2	300 m/s^{2}		Type II
Sand Dust	5S2	0,1 g/m^{3} 3,0 mg/(m^{2} · h)		

The classification according to IEC 60721-3-5 is as follows: 5K3/5B2/5S2/5M2.

IEC 60721-3-5 does not specify conditions for fog. If fog turns out to be a critical influence for the SRS/SRSS, additional sources (e.g. weather archives) shall be used to specify limit values.

Due to the motion of the vehicle, splash water shall be considered.

It can be expected that, upon entering or leaving an indoor environment, rapid temperature and humidity changes occur. This might give rise to condensation on the SRS/SRSS. The effects of condensation on the dependability of detection shall be considered.

F.3 Example 2 for application of environmental influences

A stationary camera based SRS/SRSS is used to monitor a semi-sheltered entrance area of a factory building. The SRS/SRSS as well as the sensing zone is exposed to outdoor climate but sheltered from the direct influences of precipitation and sunlight.

An analysis has identified the following relevant environmental influences for the SRS/SRSS:

- temperature and humidity;
- fog;
- condensation and icing;
- indirect solar radiation;
- dust and sand;
- vibration and shocks;
- electrical and electromagnetic influences.

Not listed items out of the list of environmental influence in accordance with 5.8.3.2 are irrelevant and have been omitted.

Relevant parts of the IEC 60721 (all parts) are IEC 60721-3-0 (Introduction) and IEC 60721-3-3 (Stationary use at weather-protected locations).

For simplicity, storage conditions are neglected in this example.

Resulting environmental influences relevant for the detection according to classification and application specific modifications are listed in the following Table F.2.

Table F.2 – Example 2 of environmental influence and classes according to IEC 60721-3-3

Environmental influence	Class according to IEC 60721-3-3	Limits	Modification of limits	Remarks
Temperature	3K6	–25 °C to +55 °C		
Change rate of temperature	3K6	0,5 K/min		
Relative humidity	3K6	100 %		
Condensation	3K6	possible		
Solar radiation		700 W/m^2		
Vibration (sinusoidal) amplitude/acceleration	3M1	0,3 mm at 2 Hz to 9 Hz 1 m/s^2 at 9 Hz to 200 Hz		
Shock (peak acceleration)	3M1	40 m/s^2		Type L

The classification according to IEC 60721-3-3 is as follows: 3K6/3M1.

Annex G
(informative)

Faults, failures and influences resulting in a loss of SRS/SRSS safety related function

G.1 General

Annex G gives information on the relationship of no failure to danger requirements in accordance with 5.8.3.3 and faults and/or failures as defined for SCS and finally for safety related systems.

Hardware electronic, software and systematic capability faults and failures of an SRS/SRSS shall be combined as independent portion as shown in Figure G.1.

Accumulated duration of failure to danger in accordance with Table 3 of 5.8.3.3 does not take into account random hardware electronic faults characterized by the PFH values (average frequency of dangerous failure per hour).

NOTE PFH values are applied to random faults and are only used as reference to quantify the limit for systematic faults related to systematic capability of an SRS/SRSS.

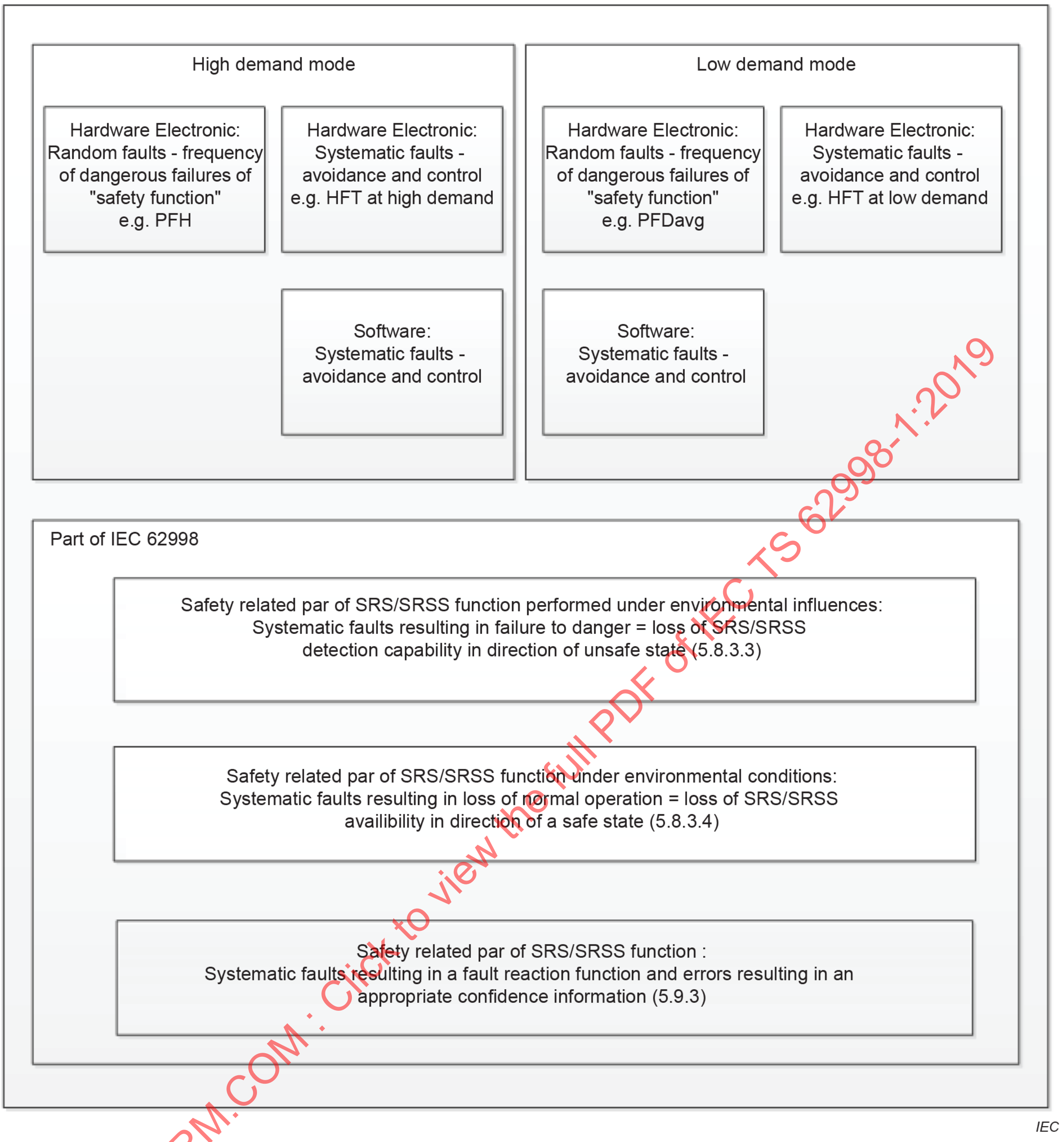

High demand mode
Hardware Electronic: Random faults - frequency of dangerous failures of "safety function" e.g. PFH
Hardware Electronic: Systematic faults - avoidance and control e.g. HFT at high demand
Software: Systematic faults - avoidance and control
Low demand mode
Hardware Electronic: Random faults - frequency of dangerous failures of "safety function" e.g. PFDavg
Hardware Electronic: Systematic faults - avoidance and control e.g. HFT at low demand
Software: Systematic faults - avoidance and control
Part of IEC 62998
Safety related par of SRS/SRSS function performed under environmental influences: Systematic faults resulting in failure to danger = loss of SRS/SRSS detection capability in direction of unsafe state (5.8.3.3)
Safety related par of SRS/SRSS function under environmental conditions: Systematic faults resulting in loss of normal operation = loss of SRS/SRSS availibility in direction of a safe state (5.8.3.4)
Safety related par of SRS/SRSS function : Systematic faults resulting in a fault reaction function and errors resulting in an appropriate confidence information (5.9.3)
IEC

Figure G.1 – Combination of faults, failures or errors resulting in additional risk throughloss of safety function or bypassing

This document give special attention to:

- systematic faults resulting in failure to danger of detection capability;
- systematic faults resulting in loss of normal operation;
- appropriate signal to initiate the fault reaction function at the output unit, and
- errors resulting in appropriate confidence information at the output unit.

The approach of complete analysis within this document to cover systematic faults resulting in a failure to danger or loss of normal operation due to a loss of detection capability is shown in Figure G.2

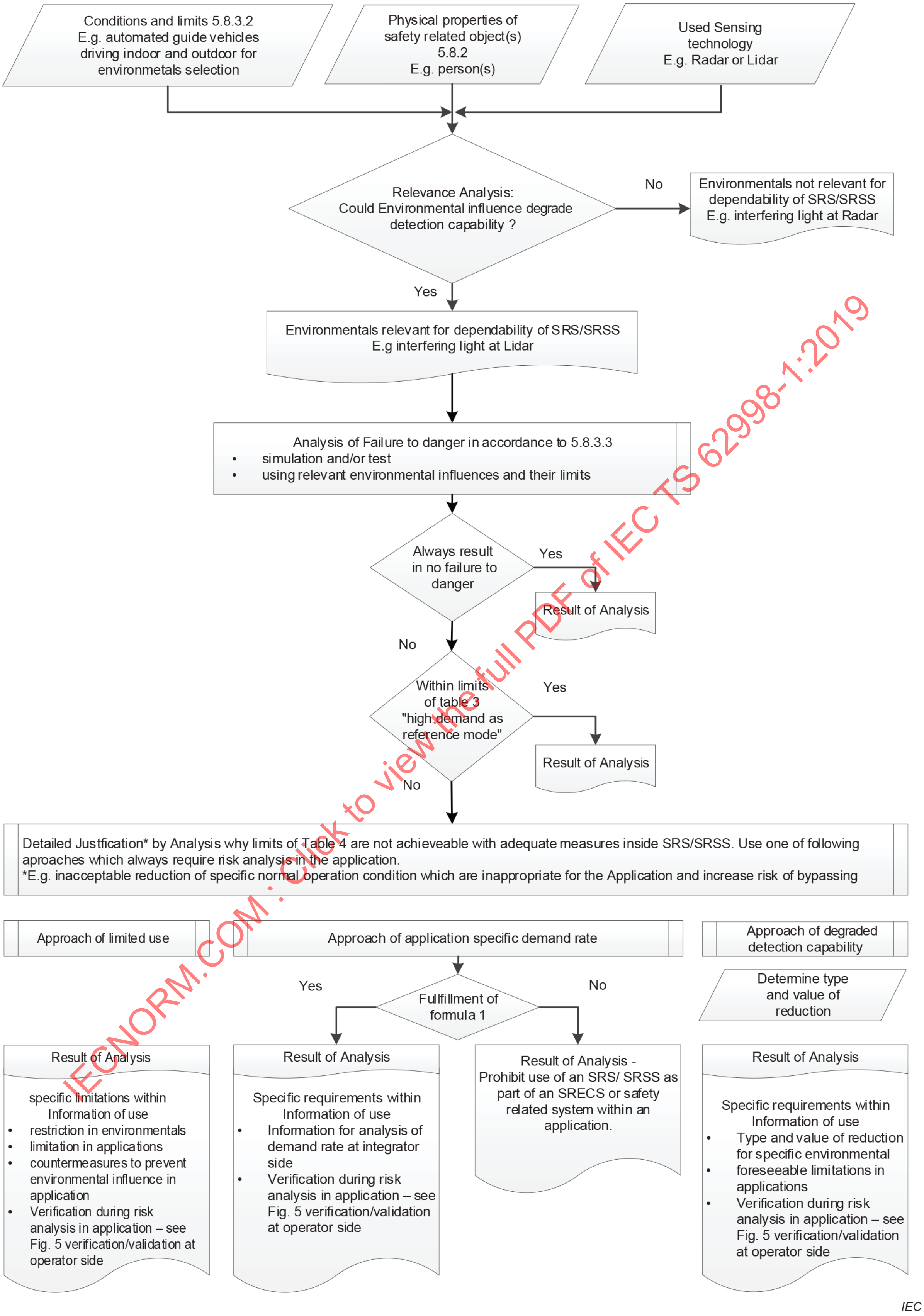

Conditions and limits 5.8.3.2
E.g. automated guide vehicles driving indoor and outdoor for environmetals selection
Physical properties of safety related object(s) 5.8.2
E.g. person(s)
Used Sensing technology
E.g. Radar or Lidar
Relevance Analysis:
Could Environmental influence degrade detection capability ?
No
Environmentals not relevant for dependability of SRS/SRSS
E.g. interfering light at Radar
Yes
Environmentals relevant for dependability of SRS/SRSS
E.g interfering light at Lidar
Analysis of Failure to danger in accordance to 5.8.3.3
• simulation and/or test
• using relevant environmental influences and their limits
Always result in no failure to danger
Yes
Result of Analysis
No
Within limits of table 3 "high demand as reference mode"
Yes
Result of Analysis
No
Detailed Justfication* by Analysis why limits of Table 4 are not achieveable with adequate measures inside SRS/SRSS. Use one of following aproaches which always require risk analysis in the application.
*E.g. inacceptable reduction of specific normal operation condition which are inappropriate for the Application and increase risk of bypassing
Approach of limited use
Approach of application specific demand rate
Approach of degraded detection capability
Yes
Fulfillment of formula 1
No
Determine type and value of reduction
Result of Analysis
specific limitations within Information of use
• restriction in environmentals
• limitation in applications
• countermeasures to prevent environmental influence in application
• Verification during risk analysis in application – see Fig. 5 verification/validation at operator side
Result of Analysis
Specific requirements within Information of use
• Information for analysis of demand rate at integrator side
• Verification during risk analysis in application – see Fig. 5 verification/validation at operator side
Result of Analysis - Prohibit use of an SRS/ SRSS as part of an SRECS or safety related system within an application.
Result of Analysis
Specific requirements within Information of use
• Type and value of reduction for specific environmental
• foreseeable limitations in applications
• Verification during risk analysis in application – see Fig. 5 verification/validation at operator side
IEC

Figure G.2 – Analysis of systematic capabilities during design and development to prevent systematic faults resulting in failure to danger

As shown in Figure G.2, there is an option in accordance with an application specific demand rate of SRS/SRSS. Predominately, a high demand mode is used as reference for definition of Table 4 for analysis of failure to danger.

G.2 Failure to danger

Systematic faults in the design (e.g. defined limits in accordance with 5.8.3.2 on relevant environmental type rain) resulting in a failure to danger due to a loss of detection capability of the SRS/SRSS safety related function shall be controlled by the requirements of 5.8.3.3.

Table G.2 is a reduced part of Table G.1 and equal to Table 4. Table G.2 shows the accumulated duration of failure and is oriented on the limit of the frequency of dangerous failures in hardware electronic.

NOTE Quantitative limit values for control and avoidance of systematic faults resulting in failure to danger are defined the first time for safety related sensors in this document. It is foreseeable that this could be not achievable in some applications and alternative approaches are needed as defined in Figure G.2.

Table G.1 – Demand rates used for the calculation of Table G.2 values

Demand rate		**1/24h**		**1/h**		**4/h**		**10/h**		**60/h**	
SRS/SRSS class	**Year/ year [a]**	**PFH**	**PL**	**PFH**	**PL**	**PFH**	**PL**	**PFH**	**PL**	**PFH**	**PL**
A	1,1E-04	4,8E-06	b	1,1E-04	none	4,6E-04	none	1,1E-03	none	6,8E-03	none
B	9,5E-06	4,0E-07	d	9,5E-06	b	3,8E-05	a	9,5E-05	a	5,7E-04	none
C	1,9E-06	7,9E-08	e	1,9E-06	c	7,6E-06	b	1,9E-05	a	1,1E-04	none
D	1,6E-07	6,6E-09	e	1,6E-07	d	6,3E-07	d	1,6E-06	c	9,5E-06	b
E	1,6E-08	6,6E-10	e	1,6E-08	e	6,3E-08	e	1,6E-07	d	9,5E-07	d

[a] Corresponds to max. accumulated duration of failure to danger per year.

not relevant

Condition in accordance with ISO 13849-1 used as reference for Table G.2

Table G.2 – Limits for failure to danger condition (loss of the detection capability) due to environmental influence for high demand mode

SRS/SRSS performance class	**Max. accumulated duration of failure to danger per year**
A	1 h
B	5 min
C	1 min
D	5 s
E	0,5 s
F	Response time

Further approaches as shown in Figure G.2 are possible if a justification show that the limits of Table G.2 are not applicable. Special attention shall be given by the manufacturer and supplier to inform the user and/or integrator in an appropriate way if these approaches are used.

Formula (G.1) shall be used if the approach of application specific demand rate shall be applied.