BS EN 50156-1:2015

BSI Standards Publication

Electrical equipment for furnaces and ancillary equipment

Part 1: Requirements for application design and installation

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 50156-1:2015. It supersedes BS EN 50156-1:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee PEL/27, Electroheating.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 78403 3

ICS 27.060.01

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2015.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50156-1

July 2015

ICS 27.060.01

Supersedes EN 50156-1:2004

English Version

Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation

Equipements électriques d'installation de chaudière - Partie 1: Règles pour la conception, pour l'application et l'installation

Elektrische Ausrüstung von Feuerungsanlagen und zugehörige Einrichtungen - Teil 1: Bestimmungen für die Anwendungsplanung und Errichtung

This European Standard was approved by CENELEC on 2015-01-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN 50156-1:2015 E

Contents

EN 50156-1:2015 (E)

European foreword

This document (EN 50156-1:2015) has been prepared by CLC/BTTF 132-2 “Revision of EN 50156 “Electrical equipment for furnaces and ancillary equipment” in cooperation with the National Committee DKE/K 232.

The following dates are fixed:

• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2016-01-26
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	2018-01-26

This document supersedes EN 50156-1:2004.

EN 50156-1:2015 includes the following significant technical changes with respect to EN 50156-1:2004:

- harmonization of the definitions to the new version of EN 61508;
- check and updating of the normative references;
- elimination of all normative references to the machinery directive 2006/42/EC;
- alignment to the requirements for safety related system to EN 12952 and EN 12953;
- modifications in Clause 10.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This standard covers the Principle Elements of the Safety Objectives for Electrical Equipment Designed for Use within Certain Voltage Limits (LVD - 2006/95/EC).

Requirements of this standard covers the essential safety requirements for limiting devices in the scope of this standard which are safety accessories in the sense of pressure equipment directive 97/23/EG, which are classified in the category II and higher.

This standard is the first part of a series of European standards which specify the requirements for equipment of safety functions for furnaces, especially safety related system to protect personnel, the furnace with ancillary equipment against hazards related to heat generation, the heated system and to operate reliably during normal conditions, and abnormal conditions which can be foreseen.

This European Standard has been prepared by the German National Committee with the participation of experts of other National Committees on the basis of CLC/BT(DE/NOT)140. It is divided into 3 parts under the generic title “*Electrical equipment for furnaces and ancillary equipment*”:

- Part 1: Requirements for application design and installation;
- Part 2: Requirements for design, development and type approval of safety-relevant equipment;
- Part 3: Requirements for plant-specific tests of safety-relevant equipment.

This European Standard is based on the EN 61508:2010 “*Functional safety of electrical/electronic/programmable electronic safety-related systems*”, Parts 1 to 7 as a basic safety standard.

Introduction

This part of the European Standard EN 50156 specifies the requirements and recommendations for the application design and installation of electrical and control equipment for furnaces and ancillary equipment and for the systems heated by the thermal energy released in the furnace to ensure:

- safety of personnel, property and the environment;
- consistency of proper function.

The operating conditions of the furnace, the hazards of combustion and the safety of heated systems are considered.

A safety-related system consisting of safety devices for:

- monitoring of flames and other safety conditions of the firing;
- interrupting the flow of fuel to the furnace;
- ventilating the body of the furnace and the flue gas ducts;
- monitoring of the safety condition of the heated systems (e.g. water level limiter in steam boilers);

may be necessary to ensure proper ignition and combustion of fuel and to avoid the development, existence and/or ignition of an explosive mixture of fuel and air, and also to avoid damage to the heated systems (see 3.25).

The rating of necessary safety integrity levels is based on EN 61508-1.

Figure 1 is provided as an aid to understanding the relationship between the various elements of furnaces and their ancillary equipment, the heated systems, the control system and the safety-related systems.

EN 50156-1:2015 (E)

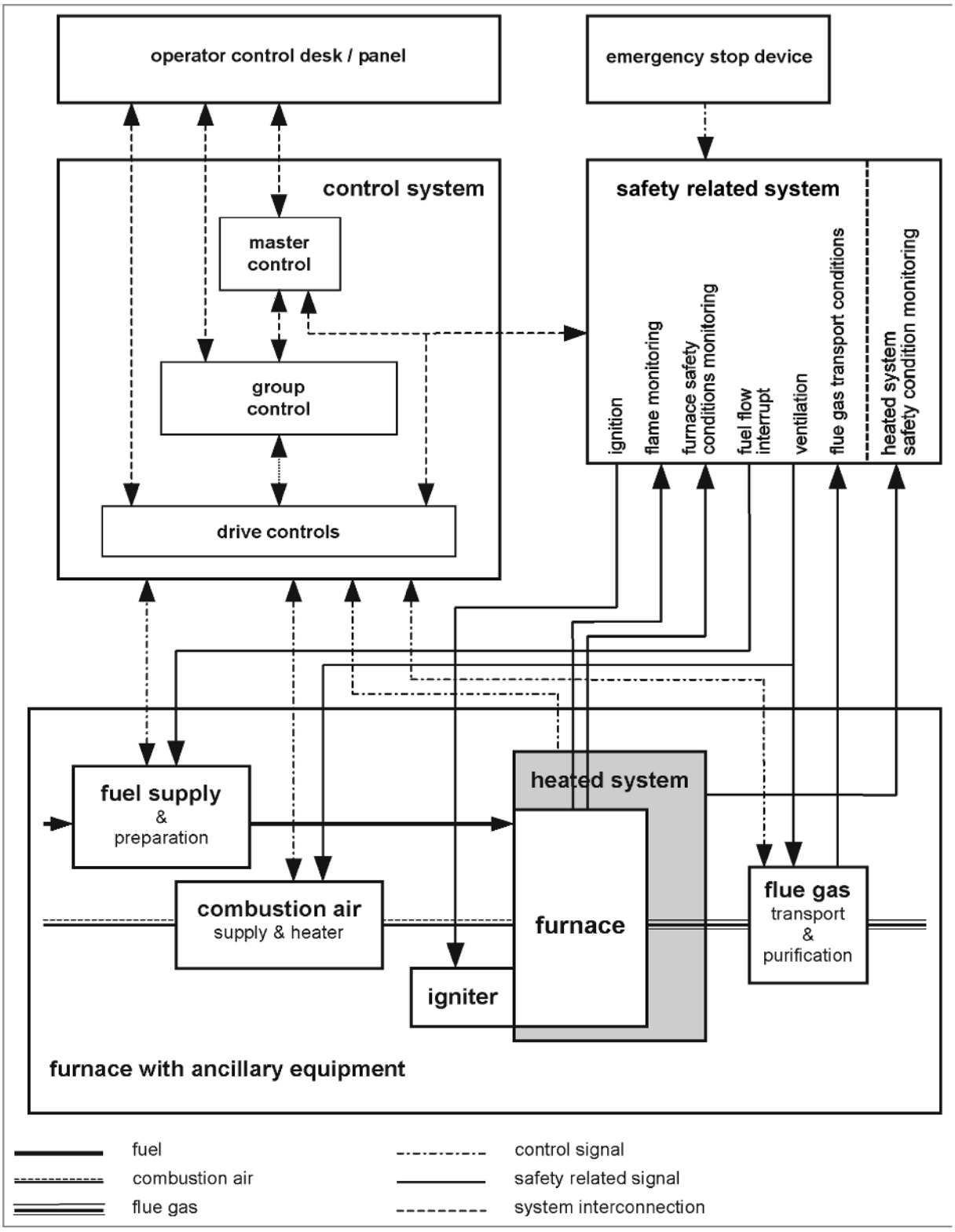


Figure 1 – Example of the functionality of a furnace with ancillary equipment, heated systems and relationship to control system and safety related system

1 Scope

This European Standard applies to the application design and installation of electrical equipment, control circuits and safety-related systems for furnaces which are operated with solid, liquid or gaseous fuels and their ancillary equipment. It specifies requirements to meet the operating conditions of furnaces, to reduce the hazards of combustion and to protect the heated systems from damage e.g. by overheating.

Such furnaces and the electrical equipment may be part by way of example of the following plant:

a) water heating systems;

b) steam boiler installations (steam and hot-water boilers) and heat recovery steam boilers;

NOTE 1 The requirements of this standard apply according to the electrical equipment of electrically heated steam boilers.

NOTE 2 Seagoing vessels and offshore facilities are governed by International Maritime Law and as such are not within the scope of this standard. These requirements may be used for such facilities.

c) warm air heaters;

d) hot-gas heaters;

e) heat exchanger systems;

f) combustion chambers of stationary turbines;

g) as long as no other standard is applicable for combined heat and power stations, we recommend the use of the requirements of this standard;

h) This standard may also be used as reference for electrical equipment requirements for thermo-processing equipment.

The requirements in this standard are not applicable to electrical equipment for:

i) non-electrically heated appliances and burner control systems for household and similar purposes;

j) furnaces using technologies for the direct conversion of heat into electrical energy;

k) combustion chambers of non-stationary prime movers and turbines;

l) central oil supply systems for individual heating appliances;

m) furnaces using solid fuels for heating purposes for household use with a nominal thermal output up to 1 MW;

n) furnaces which are used to heat process fluids and gasses in chemical plant.

This European Standard may be used as a basis for the requirements placed on electrical equipment for furnaces, which are excluded from its field of application.

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.

EN 12952-7:2012, *Water-tube boilers and auxiliary installations - Part 7: Requirements for equipment for the boiler*

EN 12952-8:2002, *Water-tube boilers and auxiliary installations - Part 8: Requirements for firing systems for liquid and gaseous fuels for the boiler*

EN 12952-9:2002, *Water-tube boilers and auxiliary installations - Part 9: Requirements for firing systems for pulverized solid fuels for the boiler*

EN 12952-16:2002, *Water-tube boilers and auxiliary installations - Part 16: Requirements for grate and fluidized-bed firing systems for solid fuels for the boiler*

EN 12953-6:2011, *Shell Boilers - Part 6: Requirements for equipment for the boiler*

EN 12953-7:2002, *Shell boilers - Part 7 : Requirements for firing systems for liquid and gaseous fuels for the boilers*

EN 12953-12:2003, *Shell boilers - Part 12: Requirements for grate firing systems for solid fuels for the boiler*

EN 55011:2009, *Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement (CISPR 11:2009, mod.)*

EN 55022:2010, *Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement (CISPR 22:2008, mod.)*

EN 60034 all parts, *Rotating electrical machines (IEC 60034-1, all parts)*

EN 60309-1:1999, *Plugs, socket-outlets and couplers for industrial purposes - Part 1: General requirements (IEC 60309-1:1999)*

EN 60332-1-1, *Tests on electric and optical fibre cables under fire conditions - Part 1-1: Test for vertical flame propagation for a single insulated wire or cable - Apparatus*

EN 60332-2-1, *Tests on electric and optical fibre cables under fire conditions - Part 2-1: Test for vertical flame propagation for a single small insulated wire or cable - Apparatus*

EN 60445:2010 , *Basic and safety principles for man-machine interface, marking and identification - Identification of equipment terminals, conductor terminations and conductors (IEC 60445:2010)*

EN 60529:1991, *Degrees of protection provided by enclosures (IP Code) (IEC 60529:1989)*

EN 60654-3:1997, *Operating conditions for industrial-process measurement and control equipment - Part 3: Mechanical influences (IEC 60654-3:1983)*

EN 60664-1:2007, *Insulation coordination for equipment within low-voltage systems - Part 1: Principles, requirements and tests (IEC 60664-1:2007)*

EN 60947-2:2006, *Low-voltage switch gear and control gear – Part 2: Circuit-breakers (IEC 60947-2:2006)*

EN 60947-3:2009, *Low-voltage switchgear and controlgear - Part 3: Switches, disconnectors, switch-disconnectors and fuse-combination units (IEC 60947-3:2008)*

EN 60947-4-1:2010, *Low-voltage switchgear and controlgear - Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters (IEC 60947-4-1:2009)*

EN 60947-5-1:2004, *Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices (IEC 60947-5-1:2003)*

EN 61000-4, all parts, *Electromagnetic compatibility (EMC) (IEC 61000-4, all parts)*

FprEN 61000-6-7:2014, *Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations (IEC 61000-4-7:201X)*

EN 61082-1:2006, *Preparation of documents used in electrotechnology - Part 1: Rules (IEC 61082-1:2006)*

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

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

EN 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6:2010)*

EN 61558-1:2005, *Safety of power transformers, power supplies, reactors and similar products - Part 1: General requirements and tests (IEC 61558-1:2005)*

EN 61810-1:2008, *Electromechanical elementary relays - Part 1: General requirements (IEC 61810-1:2008)*

HD 60364-4 (all parts), *Low-voltage electrical installations – Part 4: Protection for safety (IEC 60364-4, all parts)*

HD 60364-4-41:2007, *Low-voltage electrical installations – Part 4-41: Protection for safety – Protection against electric shock (IEC 60364-4-41:2005, modified)*

EN 81346-1, *Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations - Part 1: Basic rules (IEC 81346-1)*

IEC 60417, *Graphical symbols for use on equipment (IEC 60417 all parts)*

IEC 60536-2:1992, *Classification of electrical and electronic equipment with regard to protection against electric shock – Part 2: Guide to requirements for protection against electric shock*

IEC 60617, *Graphical symbols for diagrams*

ISO 3864, *Safety colours and safety signs*

3 Terms and definitions

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

3.1
actuating element
component which produces changes in other electrical circuits or volume flows (e.g. fuel, air) as a result of the effect of changes in signal

Note 1 to entry: Examples are valves, switches and motors including their common auxiliaries, also for example solenoid valve with magnetic actuation and final control element for direct process control

EN 50156-1:2015 (E)

3.2
auxiliary circuit
electrical circuit for ancillary functions, e.g. control circuits (command initiation, interlocking operation), signalling and measuring circuits

3.3
certificate of conformity
declarations that the equipment is in accordance with the relevant standard (see 10.7.3)

Note 1 to entry: In some legislation these declarations are only accepted from independent assessors depending on the required safety integrity level.

3.4
component
constituent part of electrical devices or subsystems, usually specified by function, but used in various applications. These are elements or components in the sense of EN 61508-4. Examples include resistors, capacitors, transistors, integrated circuits, printed-circuit boards

Note 1 to entry: A component is the smallest element a circuit can be subdivided into. If a component has to be broken down it loses its physical characteristics and/or does not conform to specifications.

Note 2 to entry: An element may comprise hardware and/or software.

3.5
proven in use
demonstration, based on an analysis of operational experience for specific configuration, an element that likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required safety integrity level

3.6
continuous operation
operation can be maintained for longer than 24 h without interruption

3.7
control circuit
electrical circuit used for the operational control and the protection of the furnace and of the power circuits

3.8
control device
device connected into the control circuit and used for controlling the operation of the furnace. For example, a manually operated switch, a limit transducer, or a valve

3.9
current limiting
limiting of electric current to a predetermined maximum value for the defined operation by means of a suitable arrangement of components in the circuit

3.10
Diagnostic Coverage
DC
proportion of all hardware faults which are detected by the online diagnostics embedded in the safety-related system

Note 1 to entry: To determine the DC a fault model should be used which is sufficient for the concerned technology.

3.11
diverse programs (software)
programs or program sections which represent different solutions to an identical task which were either written (independently) by various persons or take different approaches to problems from the outset to achieve the same result (design diversity)

3.12
electrical equipment
equipment for furnaces includes all electrical equipment for the fields of application mentioned in Clause 1

3.13
emergency stop device
manually operated switch which can be used to shut down the furnace and its associated equipment in the event of danger. The emergency stop device shall prevent fuel flow and electrical preheating

Note 1 to entry: In EN 12952–8 and EN 12952–9 the emergency stop is defined as master fuel trip (MFT).

3.14
external diagnostic
ED
measures to detect failures, particularly passive failures, where additional devices, which do not form part of the programmable controller or one of its channels, are used to test the function of particular sections or the entire programmable controller. The external diagnostic may be performed by another channel in the case of a multi-channel configuration

3.15
external influences
influences from the environment which could bring about a failure or malfunction of the function

Note 1 to entry: The following are examples of external influences on electrical systems:

a) Power failure and return of power, over-voltage and under-voltage, short-power interruptions (<0,5 s).

b) Electromagnetic and electrical disturbances, such as inductive or capacitive interference or leakage currents through resistive connections.

c) For microelectronic components, ionising radiation.

3.16
Failure
F
termination of the ability of an item to perform 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.

[SOURCE: IEC 60050-191:1990, definition 191-04-01]

3.17
failure mechanism
physical or chemical process which causes an assembly to fail. It may also define how the assembly fails, e.g. fail to safety. In doing so it may be possible to detect a failure tendency direction

3.18
fault
state of an item characterised by inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources e.g. loss of power supplied (see Figures 2 and 3)

Note 1 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure (191–05–01 of IEC 60050–191:1990).

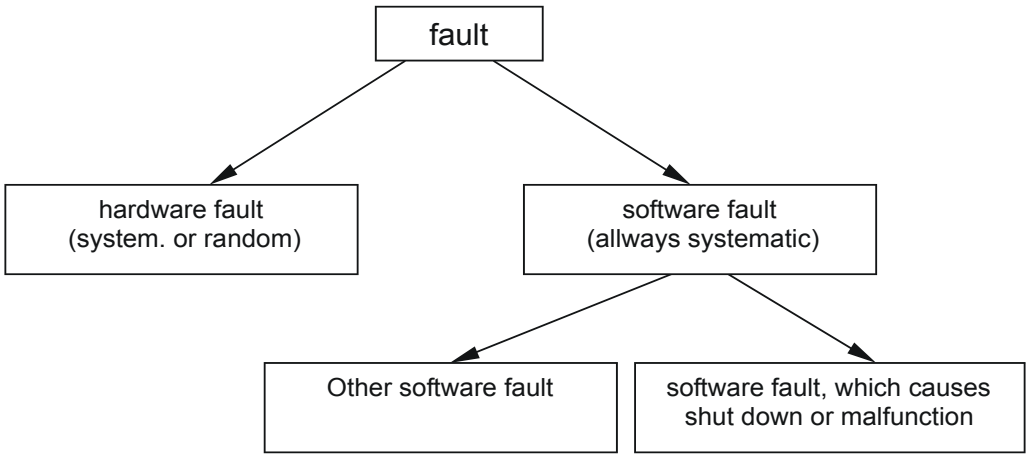


Figure 2 – Types of faults to be considered

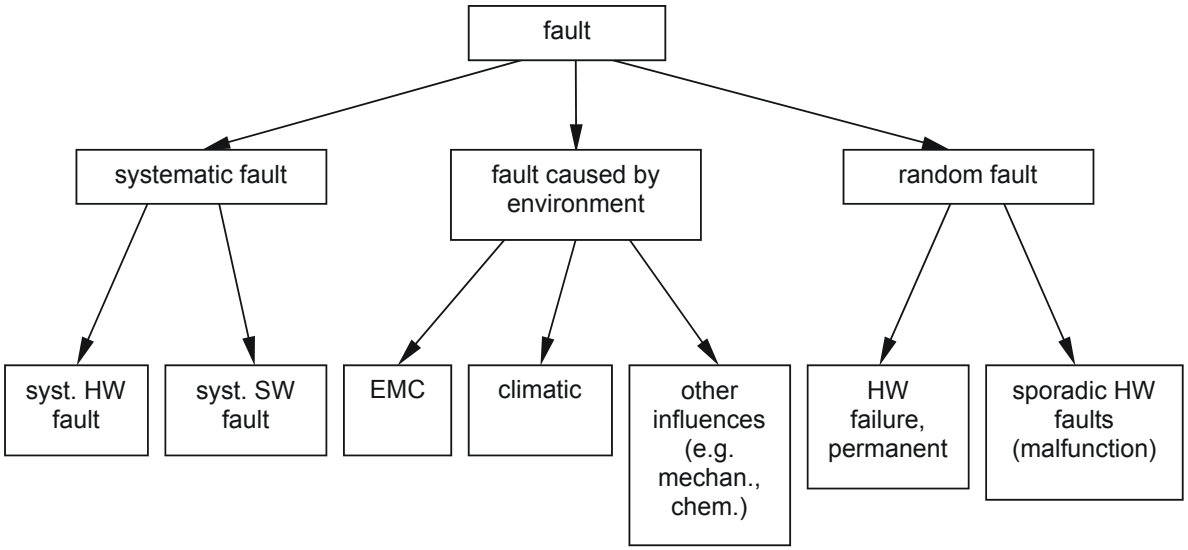


Figure 3 – Causes of faults to be considered

3.19
fault exclusion
exclusion of a theoretically possible fault whose occurrence, in the light of practical experience, or under the given physical conditions is so unlikely, that it needs not to be taken into account

3.20
fault tolerance time
time between the occurrence of an unsafe condition (caused by the process itself or due to equipment failure) and the point when the process changes into critical operation, which would result in an hazardous event in the absence of any safety-related systems

3.21
flame monitoring device or unit
safety device which is triggered by the presence or absence of flame and gives an appropriate signal to the protective equipment

3.22
function test
complete test of an individual safety-related function. This includes testing as to whether the safety-related system (sensors, protective equipment and actuating elements) is acting correctly when a process parameter is changed to ensure correct operation of the safety-related function

Note 1 to entry: Function tests of the complete safety-related functions may be carried out by overlapping partial tests.

3.23
furnace
structure within which heat is generated to a controlled temperature by combustion of fuel

Note 1 to entry: The English term „furnace“ includes structures within which heat is generated by electricity and other forms of energy. This standard also applies to the electrical equipment of electrically heated or heat recovery steam boilers.

3.24
furnace and ancillary equipment
this includes all the equipment for the burning of fuels, for example, equipment for the storage, preparation and transport of fuels, combustion air supply[1)], cleaning and removal of flue gas and exhausts and relevant closed-loop and open-loop control and monitoring equipment

3.25
heated system
equipment which absorbs the heat generated in the furnaces, e.g. economiser, evaporator, and superheater of a steam boiler, heat exchanger, gas turbine

3.26
immersion electrode
limit transducer for fluid level monitoring

3.27
logic unit
safety-related control and switching equipment which receives signals from sensors, limiters and other monitoring devices. Its purpose is to control actuating elements according to the specified safety function

Note 1 to entry: Protective equipment may consist of a completely hard-wired device or it may be a programmable safety device incorporating electronics and a programming facility. In hard-wired equipment, the signals from all modules are generated and processed by individual connections. In programmable safety devices, signals are processed by means of programs (software) stored in memories.

3.28
main circuit
electrical circuit which supplies the electrical energy to equipment for the generation, conversion, distribution, switching and consumption of electrical energy

3.29
Malfunction
M
transient fault

3.30
management of faults
all measures which ensure that when a fault occurs the system remains in a safe state or that a safe state is achieved

---

1) Also applies to gas turbines containing oxygen within its exhaust gas.

3.31
non-opening of contact elements
fault which prevents the opening of contacts of relays or other switching devices e.g. contact welding, sticking of the magnet armature, etc

3.32
Program Analysis
PA
all measures used in the context of theoretical checking to reveal software errors

3.33
programmable controller
device with binary logic elements which responds to control devices and initiates a specific programmed sequence

3.34
Programmable Safety Device
PSD
programmable component within the protective equipment

3.35
Proof Of Correctness
POC
verification that the safety related program functions have been fulfilled

3.36
protective bonding circuit
protective conductors and conductive parts used to protect against the consequences of earth faults

3.37
protective conductor
conductor required by some measures for protection against electric shock for electrically connecting any of the following parts:

- exposed conductive parts;
- extraneous conductive parts;
- main earthing terminal

3.38
safety-related system
all equipment, units and safety-related circuits whose main purpose is the protection of personnel, property or the environment. The safety-related system includes all the components required to carry out the safety function, for example, sensors which monitor safety-related parameters (e.g. flame monitoring), interruption device for the flow of fuel, ventilation of the body of the furnace and protection of the heated system (e.g. monitoring the water level of steam boilers). Typically a safety-related system consists of sensors, logic solving protective equipment and actuating elements (see Figure 4). If this is achieved by multi-channel systems, then all channels and monitoring devices used for safety purposes are included within the safety-related system

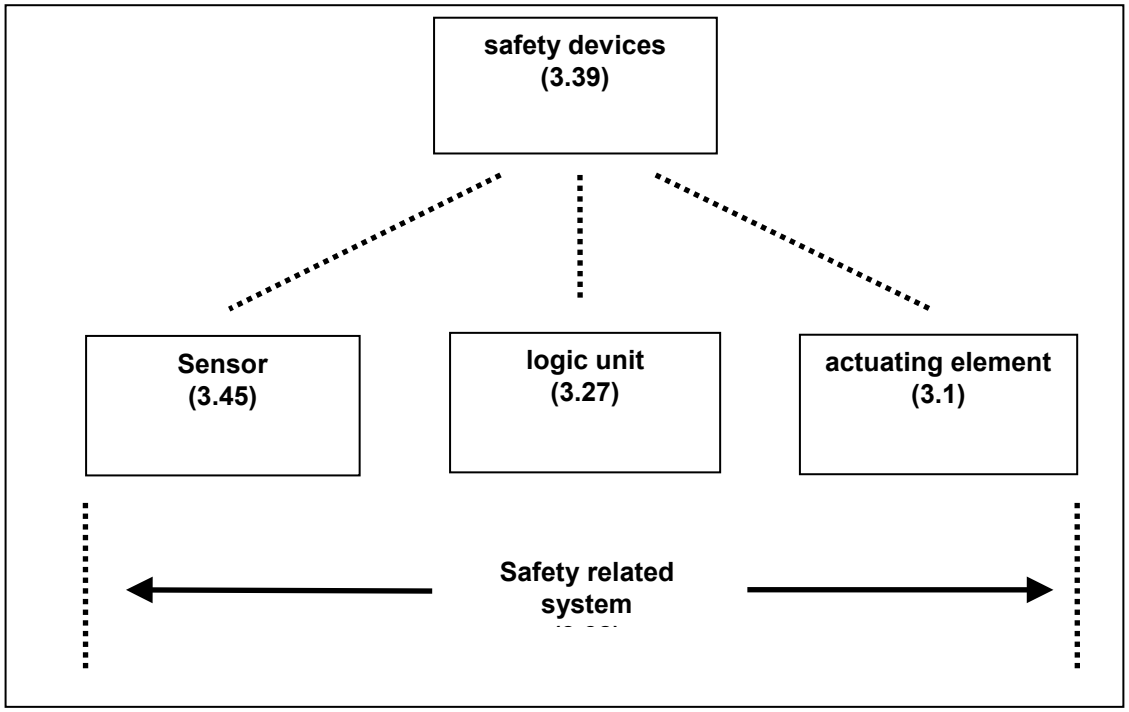


Figure 4 – Definition and components of a safety-related system

3.39
safety device
any device which is used to carry out safety functions, either on its own or as a part of a safety-related system (e.g. sensors, limiters, flame monitors, burner control devices, logic system, actuating elements, fuel shut down valves etc.). Safety devices are subsystems in terms of EN 61508-4

3.40
safety function
function to be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event

[SOURCE: EN 61508-4:2010, 3.5.1]

3.41
safety integrity
probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time

3.42
Safety Integrity Level
SIL
there are 4 possible discrete levels for specifying the safety integrity requirements of the safety function to be allocated to the safety-related systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest

3.43
safety time
safety time of a furnace is the time taken (lower part of Figure 13) from the occurrence of an unsafe operating condition (for example, flame interrupt during normal operation) to the point at which the actuating element is initiated. The reaction time of the actuating element is to be considered separately

Note 1 to entry: The response times of actuators are partly defined in the standards for the products and applications.

EN 50156-1:2015 (E)

3.44
self diagnostic
SD
measures to detect failures where additional programs in the programmable safety device (PSD) are used to test the function of specific components (e.g. ROM) or functional modules (e.g. I/O modules) which belong to the programmable controller or to one of its channels

3.45
sensor
element or device which collects an indicated value (e.g.: measuring element, transducer, transformer, limit switch)

3.46
software
SW
software includes programs, parameters and data. The software is made up of application software and system software (see Figure 5)

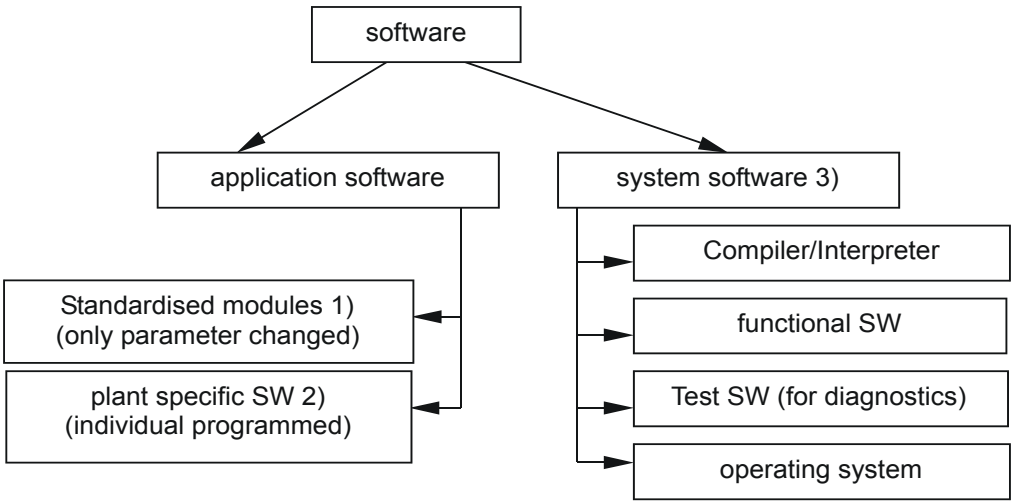


Figure 5 – Software

Note 1 to entry: Type approval according to Part 2 of this Standard, test of correctness of parameter setting (application related) according to Part 3 of this Standard.

Note 2 to entry: Application-related approval according to Part 3 of this Standard.

Note 3 to entry: Type approval according to Part 2 of this Standard.

3.47
software faults
discrepancies between program functions performed in the program and the specified program functions (see also Figures 3 and 4)

Note 1 to entry: All software errors are systematic errors.

3.48
software test (T)
measures to reveal software errors where the input interfaces of the program modules or the entire program is supplied with input data records and program execution and results (output data) are captured and compared with those obtained on the basis of the specification or program analysis

3.49
systematic hardware faults
faults in the equipment under consideration caused by inadequate specifications or errors in design, manufacturing, installation or maintenance

3.50
type approval
independent examination to ensure that a duly identified product, process or service is in conformity with a specific standard and/or the specified requirements (see 10.7.3)

3.51
validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

Note 1 to entry: In the context of this European Standard, validation means the process of demonstrating that the safety-related system under consideration, and after installation, satisfies in all respects the safety requirements specification for that safety-related system. Therefore, for example, Software Validation means confirming by examination and provision of objective evidence that the software satisfies the Software Safety Requirements Specification.

3.52
verification
confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled

Note 1 to entry: In the context of this European Standard, verification means the process of demonstrating for each phase of the relevant Safety Lifecycle (see Figure 8) by analysis and/or tests, that, for the specific inputs, the deliverables satisfy in all respects the Objectives and Requirements set for the specific phase.

Note 2 to entry: Examples of verification activities would include:

- Reviews on deliverables (documents from all phases of the Safety Lifecycle) to ensure compliance with the Objectives and Requirements of the phase taking into account the specific inputs to that phase.

- Design reviews.

- Tests performed on the designed products to ensure that they perform according to their specification.

- Integration tests performed where different parts of a system are put together in a step by step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

[SOURCE: EN 61508-4:2010, 3.5.1]

4 General requirements

4.1 General considerations

The relevant European Standards for electrical equipment apply to the installation of the electrical part of furnaces. Clause 2 lists appropriate standards and other technical codes.

Risks associated with the hazards relevant to the electrical equipment shall be assessed as part of the overall requirements for assessment of the furnace or boiler plant. This risk assessment shall be carried out for each individual situation.

The risk assessment includes the following elements for which the standard gives guidance:

a) hazard identification;

b) determine the probability of all hazards;

c) evaluate the risk(s); and

d) consider measures for risk reduction.

This will determine the acceptable level of risk and the necessary protective measures for persons who may be exposed to the hazards of the furnace and the system heated by it (e.g. steam boiler).

Hazards can include but are not limited to the following:

- electrical shock or electrical fire resulting from failures or faults in the electrical equipment;
- malfunctioning of the furnace resulting from failures or faults in control circuits (or components and devices associated with these circuits);
- malfunctioning of the furnace resulting from disturbances or disruptions in external power sources as well as failures or faults in the power circuits;
- electrical disturbances (e.g. electromagnetic, electrostatic, radio disturbance) either from outside the electrical equipment or internally generated;
- stored energy (either electrical or mechanical);
- burns or heat stress or damage or malfunction of parts of the electrical equipment caused by extreme temperatures of parts of the plant or in their vicinity;
- operation outside the design limits of the furnace and its associated equipment;
- incorrect combustion conditions resulting in an explosion in the furnace, the fuel or flue gas paths;
- incorrect operating condition resulting in damage to the heated system (e.g. explosion of a steam boiler caused by water level below minimum);
- unpurged furnaces in standby mode in case of a sudden ignition.

A combination of measures are necessary at the stages of design, installation and operation for protection against the hazards of the furnace and its electrical equipment.

4.2 Environmental requirements

4.2.1 General

The electrical equipment shall be selected and mounted so that it withstands the potential electrical, chemical, thermal and mechanical stresses at its place of use as well as external influences e.g. environmental stresses.

4.2.2 Environmental and operating conditions

The electrical equipment shall be suitable for use in the environmental and operating conditions as specified below.

An agreement is required between supplier and user, if the environmental and operating conditions are outside those specified below.

4.2.3 Electromagnetic compatibility

4.2.3.1 Electromagnetic compatibility – Emission requirements

The electrical interference generated by the equipment itself shall not exceed levels specified in the relevant equipment standard and other standards with electromagnetic compatibility (EMC). For permissible limits see

EN 61000-6-4 and methods of measurement of radio interference characteristics see EN 55011 or EN 55022 depending on the application.

4.2.3.2 Electromagnetic compatibility – Immunity requirements

Test instrumentation, test set-up and test procedure shall be in accordance with the relevant parts of EN 61000-4 series, the severity levels being at least level 3 and the performance criteria as specified below. The equipment under test (EUT) shall be operated at rated voltage unless otherwise specified. The equipment shall be tested during stand-by, running and lock-out condition.

Higher EMC levels may be selected depending on the environment in which the equipment is used. In these cases the appropriate levels should be used. The levels as mentioned in EN 61000-6-4 are preferred. Whenever the levels are not defined in the EN 61000-6-4 standard, they should be pre-defined between manufacturer and test house.

For functional safety requirements, FprEN 61000-6-7:2014 shall be considered.

4.2.3.3 Performance criteria

4.2.3.3.1 Safety-related functions

When tested in accordance with 4.2.3.2, safety relevant functions shall remain operational in accordance with the manufacturer's specifications. Furthermore, the equipment shall not reset when tested in lock-out condition.

4.2.3.3.2 Non-safety relevant aspects

Non-safety relevant functions shall meet the requirements as intended under the EMC-Directive. Therefore, the performance criteria of these functions shall be in accordance with the manufacturer's specifications. These specifications shall be predefined.

4.2.4 Ambient temperature

Electrical equipment shall be capable of operating correctly under the ambient temperature prevailing at the place of use.

Normally the following ambient temperatures shall be considered:

- electrical installation rooms: Electrical equipment shall be capable of operating correctly in ambient temperatures between +5 °C and +40 °C;

- plant environment (e.g. boiler house): Electrical equipment shall be capable of operating correctly in ambient temperatures between +0 °C and +55 °C;

- outdoor installation: Electrical equipment shall be capable of operating correctly in ambient temperatures between –25 °C and +40 °C.

Electrical equipment shall be designed such that it withstands temperatures from –25 °C to +70 °C during transport and storage.

If other temperatures than those specified above are expected at the place of use (e.g. upper level boiler area) electrical equipment shall be designed such that it is capable of operating correctly under these conditions. The operating temperature range shall be indicated. If the equipment is designed to be cooled while in use, the permissible coolant temperatures shall be indicated on the type plate.

4.2.5 Humidity

The electrical equipment shall be capable of operating correctly within a relative humidity range of 30 % to 95 % (non-condensing).

4.2.6 Contamination

Electrical equipment shall be adequately protected against the ingress of solid bodies and liquids (see 7.1 and 7.2).

4.2.7 Vibration and shock

Undesirable effects of vibration and shock (including those generated by the plant and its associated equipment and those created by the physical environment) shall be avoided by the selection of suitable equipment, by mounting it away from the sources of vibration, or by the use of anti-vibration mountings. A special agreement may be necessary between the supplier and the user. The minimum requirements according to EN 60654-3, classes VL 3, VH 3 and VS 3 shall be fulfilled.

4.2.8 Equipment used in flammable atmospheres

In areas where the occurrence of ignitable mixtures of gaseous fuel or combustible dust in the air may occur (e.g. gas pressure reducing stations), the relevant legislation and standards for explosion-protected electrical equipment shall be fulfilled.

In the vicinity of the furnace, where combustion takes place and hot surfaces might ignite gas-air mixtures, the occurrence of such mixtures shall be avoided, e.g. by proper venting.

4.3 Power supply

4.3.1 General

The electrical equipment shall be designed to operate correctly under the following supply conditions:

a) In the event of voltage fluctuations within a voltage range of 85 % to 110 % of the nominal voltage (mains a.c. voltage). In the case of battery operation, voltage fluctuations within a voltage range of 85 % to 120 % of the rated voltage shall be regarded as normal.

NOTE See EN 50160.

4.3.2 Power stations

In steam boiler installations, which are part of power stations, shunt faults in the installation of the generator or start up of big three phase current actuators may require the additional following conditions:

a) In the event of voltage superimposition above the limits specified under heading a) of up to 10 % of the nominal voltage in the case of a.c. voltage and up to 15 % of the nominal voltage in the case of d.c. voltage.

b) In the event of fluctuations of frequency in a frequency range of 95 % to 105 % of the nominal frequency. Different arrangements may be necessary for station-service plant in power stations.

The ranges may be reduced following agreement between the supplier and the user. The ranges specified may be exceeded if all equipment is suitable for this.

5 Incoming supply connections and devices for disconnecting and emergency stop

5.1 Incoming supply and equipment connections

5.1.1 Types of connection

One of the following types of connection shall be selected for the connection of the electrical equipment for a furnace to the incoming supply:

a) connection via permanently installed cables;

b) connection via flexible cords which are permanently connected to the supply system and the terminals of the installation;

c) connection via flexible cords which are permanently connected to the equipment and which are connected to the supply system by a plug-and-socket combination;

d) for connection to the incoming supply, only polarized plug-and-socket combination as specified in EN 60309-1 shall be used. Control or safety circuits shall be supplied directly from the incoming supply via plug-and-socket combination.

In the case of ships, only types of connection a) and b) shall be used for the primary supply of electrical equipment for the furnace from the incoming supply.

5.1.2 Terminations

5.1.2.1 General

The connecting points shall be suitable for the cross-sectional area and type of conductors to be connected.

5.1.2.2 Incoming supply terminals

The incoming supply terminals shall be unambiguously marked in accordance with EN 60445. The designations shall be consistent with the circuit documentation.

5.1.2.3 Connections to remote electrical equipment

5.1.2.3.1 General

Terminals, plug-and-socket devices or equivalent connections shall be provided in the control cabinet, in burner controls or in a special terminal box for the connection of each item of remote electrical equipment. Their designations shall be consistent with the circuit diagram.

5.1.2.3.2 Protective conductor terminal

An adequate number and design of connections shall be provided for the protective conductors (green/yellow colour coding) in the control cabinet or terminal box so that incoming or outgoing protective conductors can be individually connected. The protective conductor connections of the equipment shall be secured to prevent accidental loosening and shall be marked in accordance with EN 60445.

5.1.2.3.3 Plug-and-socket combination

If the plug-and-socket combination are not located in electrical installation rooms (where access is restricted to authorized staff) they shall be polarized and of the retaining type to prevent accidental disconnection.

On ships, all plug-and-socket combinations shall be of a retaining type and polarized.

5.2 Devices for disconnecting power supplies

5.2.1 General

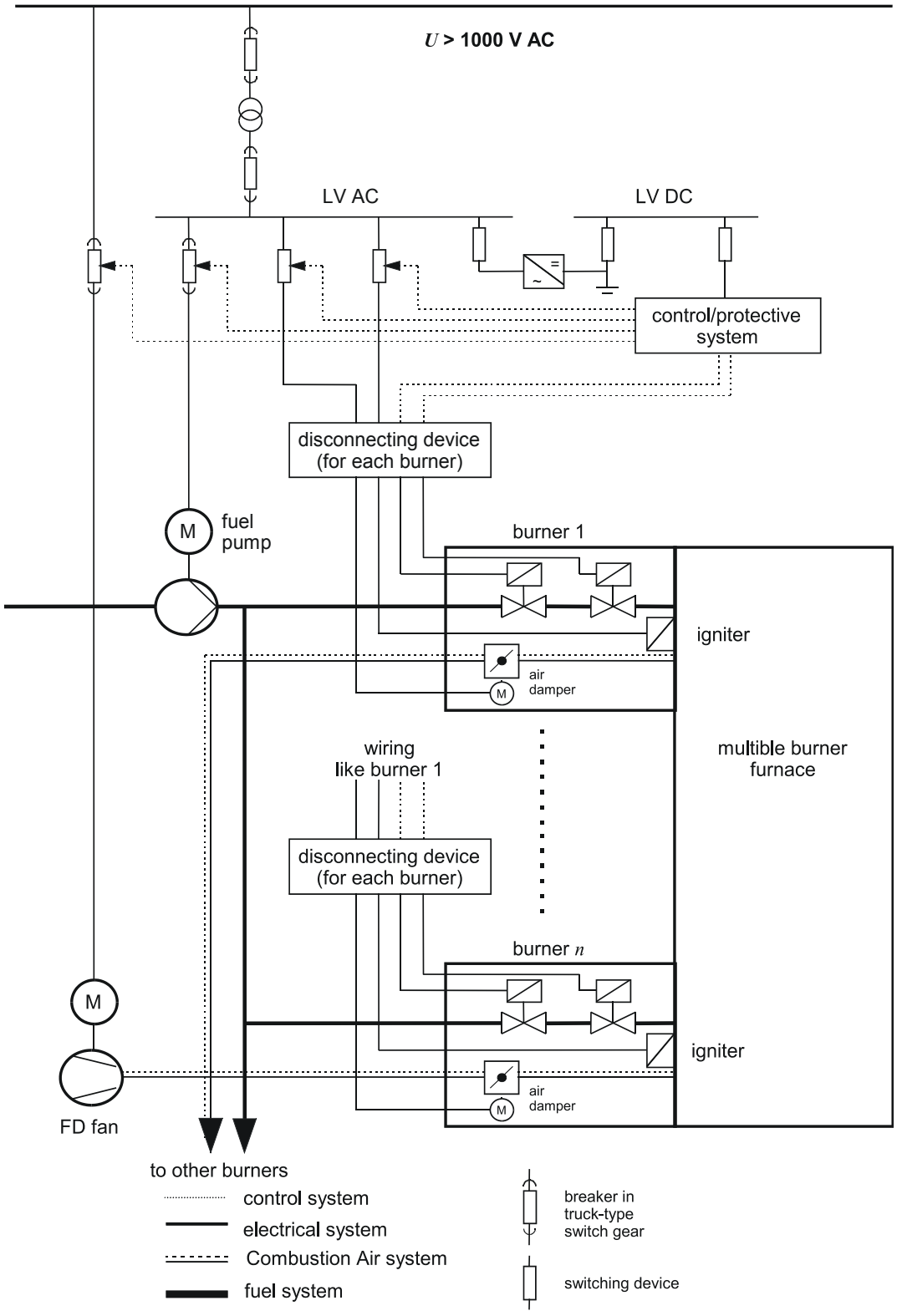


Figure 6 – Example of power supply, switching, isolating devices and other electrical components of a furnace

There shall be a supply disconnecting device which may be used to isolate the electrical equipment where necessary, for example, for cleaning, maintenance and repair works.

In the case of smaller plants, this may be achieved by a common incoming supply switch-disconnector.

In the case of large furnace, isolation shall be possible for each particular device or in groups.

Medium voltage supplies and loads shall be isolated by disconnecting switches or moving the breaker of truck-type switch gear into the disconnected position, and applying an earth.

5.2.2 Disconnecting switch

For low voltage, the disconnecting switch shall satisfy the following requirements:

- It shall be designed at least as an on-load switch in accordance with EN 60947-3;

- It shall be designed for the total current of all load circuits which can be operated simultaneously;

- It shall be possible to operate the switch manually and it shall have only **one off** and **one on** position with appropriate stops. The switch positions shall be marked in accordance to EN 60947-3;

- It shall disconnect all non-earthed conductors simultaneously and shall have disconnecting characteristics as specified in EN 60947-3. In order to avoid unauthorised operation the switch shall be capable of being locked off or adequate organisational measures shall be taken;

- It shall have a visible isolating point or a position indicator. The off position shall only be indicated when the clearances between all switch contacts stipulated in EN 60947-3 have been reached;

- If different parts of the furnace are powered from different input supply systems, it shall at least be possible to isolate them individually (see Figure 6);

- For each burner of furnaces which use solid, liquid or gaseous fuels, there shall be a disconnecting device which can be used to isolate all the electrical equipment of the burner as necessary, for cleaning, maintenance and repair work etc. as well as in the event of lengthy periods of non-use. However, in furnaces with several burners, a common disconnecting device may be used.

5.2.3 Excluded circuits

The following circuits need not be isolated by this disconnecting switch:

- lighting and socket-outlet circuits for accessories used for repairs or maintenance;

- circuits up to 50 V;

- auxiliary circuits above 50 V which are required to remain energised;

- auxiliary circuits above 50 V which permit maintenance or repair operation and auxiliary circuits for devices which make equipment inactive or inert.

These circuits shall be specially marked. Conductors for the circuits shall be routed separately and shall be routed via terminals shrouded to IP2X according to EN 60529.

Those circuits which are not switched off by the isolating device shall be detailed in the circuit documentation. An appropriate warning notice shall then be affixed to the isolating device (e.g. Warning! Auxiliary circuits remain live after disconnection).

5.3 Emergency stop

5.3.1 General

In order to reduce the risk of hazards causing injury to persons, damage to equipment or work in progress, emergency stop is necessary. The requirements for this emergency stop depend on the type of hazard and plant.

The emergency stop shall be initiated by a manually operated emergency stop device.

To reach a safe status of a furnace it is necessary to stop the energy conversion in it. That means the supply of fuel or other form of energy to the furnace has to be interrupted as fast as possible.

For machinery related to furnaces which is subject to the Machinery Directive 2006/42/EC, the standard EN ISO 13850 for emergency stop of the machine should be applied if the risk analysis of the machinery demands an emergency stop.

5.3.2 Emergency stop device for furnaces in heating installations

It shall be possible to initiate the emergency stop of oil- and gas-fired furnaces in heating installations having a nominal thermal output exceeding 50 kW by a single human action.

5.3.3 Emergency stop device for other furnaces, e.g. steam boilers

An emergency stop device shall be provided to initiate the emergency stop by a single human action in the event of a hazardous situation arising.

The emergency stop device shall directly or indirectly switch those circuits and electrical equipment of a furnace which need to be switched off to prevent an hazardous situation occurring. The emergency stop device may be integrated into the safety-related system. In that case the safety-related system and the emergency stop device functionality shall satisfy the requirements of chapter 10.

The emergency stop devices shall meet the following conditions:

- the contact members shall ensure positive opening operation (see EN 60947-5-1:2004, Annex K);

- they shall be located in an easily accessible and non-hazardous position either outside the room where the furnace is installed or along the emergency exit route and their purpose appropriately marked;

- the initiator of the emergency stop device shall be coloured red and the surface behind it shall be coloured yellow.

5.3.4 Application as isolating switch

The emergency stop device may be used as a supply disconnecting device, if it meets the conditions specified in 5.2.

6 Protection against electric shock

6.1 Protection against direct contact

The live parts of electrical equipment shall be protected against direct contact in accordance with HD 60364-4-41. Deviations or additions thereto are as follows:

a) Electrical equipment which is used outside of electrical operating areas or closed electrical operating areas shall also be protected against direct contact in the case of nominal voltages below 50 V;

b) It shall only be possible to remove or open the barriers (doors, covers) of live parts of ignition transformers and ignition electrodes by using a tool;

c) In the case of burners with high-voltage ignition which swivel out or move out, the voltage supply for the high-voltage section shall be automatically switched off when the burner is swivelled out or moved out.

NOTE Equipment designation and the application of warning signs is dealt with in Clause 13.

6.2 Protection against indirect contact

The measures in HD 60364-4-41 shall be taken as protection against indirect contact.

NOTE Structural parts of the burner, boiler or boiler room may be used as protective conductors if the conditions in HD 60364–5-54:2011, Clause 5 (Annex C) are met.

In ignition circuits, the centre tap or one pole of the high-voltage winding of the ignition transformer may be connected to the exposed conductive part; the exposed conductive part shall be connected to the protective conductor. In the case of ignition devices which can be moved or swivelled, the screen of the ignition cable shall be connected to the protective conductor, but shall not itself be relied on as a protective conductor, therefore an additional protective conductor is necessary.

7 Environmental protection of the equipment

7.1 Protection against ingress of solid foreign bodies

When installed, all electrical equipment shall at least meet the requirements of protection class IP4X in accordance with EN 60529.

This requirement is not applicable if the equipment is located in rooms where a particular type of protection is superfluous (e.g. air-conditioned or clean and dry rooms) or if it is accommodated in control cabinets and consoles which conform to the minimum requirements of degree of protection of IP4X in accordance with EN 60529 unless otherwise stipulated below.

7.2 Protection against water

Protection against water for the electrical equipment shall be suitable for local conditions. This can be ensured by means of an appropriate degree of protection as specified in EN 60529 or by suitable mounting.

For application on ships see IEC 60092-101.

8 Equipotential bonding

8.1 General

Equipotential bonding shall be designed such that the function provided by the safety related system is not impaired.

NOTE Equipotential bonding can be applied for various purposes such as

a) equipotential bonding as a protective measure for persons,

b) equipotential bonding for lightning protection,

c) functional equipotential bonding.

8.2 Equipotential bonding as a protective measure in case of indirect contact

To avoid hazardous touch voltages (e.g. caused by insulation failure between live parts and exposed conductive parts or formation of stray voltages) between metal parts of the plant and earth, there shall be a main equipotential bonding conductor connecting the following conductive parts:

- main protective conductor;

- main earthing conductor;
- lightning earth conductor;
- main water pipes;
- main gas pipes;
- other metal piping systems e.g. rising mains of central heating and air-conditioning systems, metal parts of building structure (as far as possible).

This equipotential bonding shall be in accordance with the relevant requirements of the HD 60364-4 series.

8.3 Equipotential bonding for the purpose of lightning protection

Lightning protection by equipotential bonding shall protect persons, electrical equipment and especially electronic devices from hazardous overvoltages. In addition to local requirements to protect the structure containing the furnace, which may be specified in local or national standards, all non-active metal parts shall be interconnected and connected to earth potential by an equipotential bonding conductor (see 8.2).

If a direct connection is not allowed for corrosion protection reasons, the connections shall be carried out via spark gaps.

In particular, where equipment is located outside of the structure, metal enclosures and conductive screens of cables shall be integrated in this equipotential bonding for lightning protection purposes.

The active parts and cable cores shall be provided with suitable lightning arrestor or over-voltage surge protection devices, if this is necessary to maintain safety.

8.4 Functional equipotential bonding

The measures of functional equipotential bonding shall ensure that voltages between various devices and plant components which could adversely affect their functioning are reduced to a sufficiently low level.

Devices, equipment and plant components which are functionally interdependent and which are located in close proximity to each other may be connected together by a separate equipotential bonding conductor in order to ensure their satisfactory functioning.

The functional equipotential bonding shall preferably be meshed (over an area) in order to reduce lightning overvoltages or faults at higher frequencies (electronic circuits). For protecting remote electronic devices (e.g. transducer), the electronics of which do not have their own earth connection (isolation between electronics and enclosures), functional equipotential bonding in a (centralised) star arrangement may be practical. At industrial frequencies, equipotential bonding in a star configuration is likewise recommended in order to avoid interference.

NOTE 1 The purpose of functional equipotential bonding is not to protect human beings against hazardous overvoltages. This protection is achieved by measures according to 8.2 and 8.3. Functional equipotential bonding includes individual earth connections, directly or via surge voltage protectors, if they serve to protect sensitive items of equipment, e.g. electronic devices.

NOTE 2 An agreement is required between the supplier and the user upon the concept of functional equipotential bonding (e.g. meshed, star configuration).

9 Auxiliary circuits

9.1 Supply to auxiliary circuits

9.1.1 Supply from 3-phase or a.c. systems

A 3-phase or a.c. system intended to supply auxiliary circuits shall have a neutral conductor. Auxiliary circuits shall only be connected between a line conductor and the neutral conductor.

The neutral conductor shall preferably be earthed. In non-earthed systems, auxiliary circuits shall be supplied from control supply transformers, and equipped with an earth leakage monitoring system.

The earth leakage monitoring system should provide automatic disconnection of the electrical supply of any circuit affected by the occurrence of an insulation failure in order to prevent a hazardous condition resulting from a touch voltage.

Disconnection in the event of a single fault is not necessary if the fault current is so low that it will not give rise to the risk of electric shock and an alarm signal is initiated. However, precautions shall be taken to guard against the risk of electric shock in the event of two faults existing simultaneously.

For this type of protection, the requirements of 413.1 of HD 60364-4-41:2007 should apply.

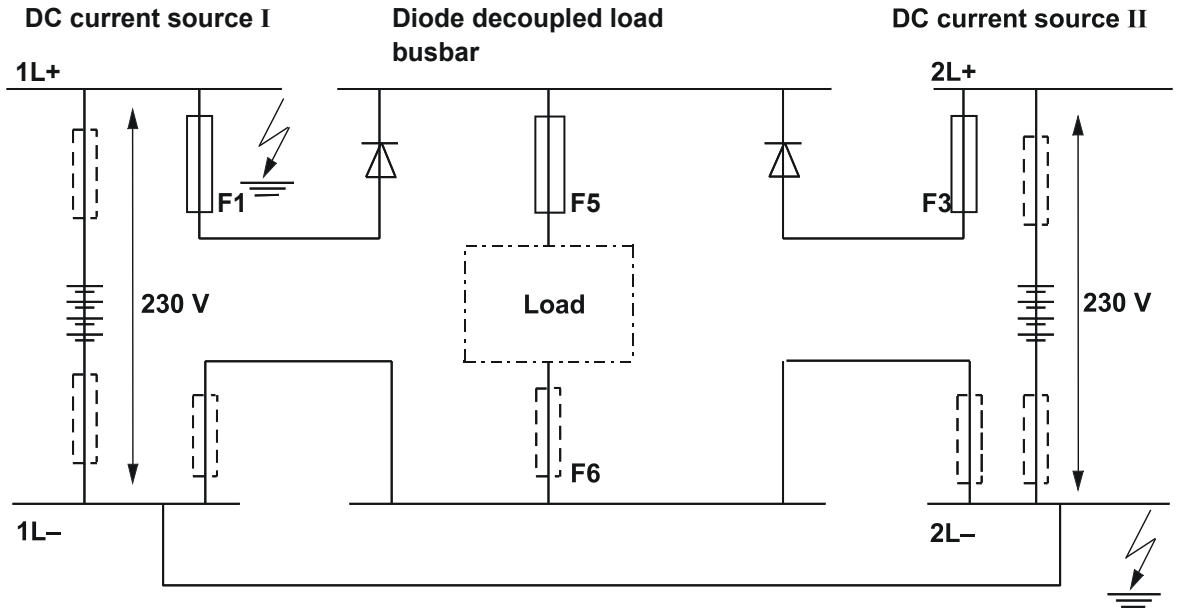
9.1.2 Supply from d.c. mains

9.1.2.1 General

With a supply from one non-earthed or single-earthed d.c. mains, the auxiliary circuit shall be connected to both poles (both line conductors).

9.1.2.2 Supply from more than one d.c. source

With a supply from more than one d.c. source with diode decoupling, the non-decoupled poles of these power sources shall additionally be directly interconnected in order to avoid voltage doubling in the event of two earth faults (see Figure 7).



With earth faults in different poles the load voltages remain unchanged.

Figure 7 – Supply from two d.c. sources

9.1.2.3 Supply from a d.c. source with an mid-point conductor

With a supply from a d.c. source with an earthed or non-earthed mid-point conductor, connection shall be made to a live conductor and the mid-point conductor.

9.1.2.4 Supply from an isolated d.c. source

Supply systems isolated from earth shall be equipped with an earth leakage monitor to prevent malfunctions in case of a dual earth fault.

9.1.3 Auxiliary circuits connected between the line conductors

If auxiliary circuits are connected between the line conductors, then the contacts of the actuating elements for safety related purposes shall switch in both line conductors or suitable measures shall be taken to prevent a functional failure of the control system in the event of a short circuit to an exposed conductive part or to earth.

9.2 Voltage for auxiliary circuits

9.2.1 Operating voltage of auxiliary circuits

Auxiliary circuits shall be operated with nominal voltages ≤ AC 400 V or ≤ DC 250 V.

This does not include flame monitors and ignition devices.

On ships, auxiliary circuits may be operated with a nominal voltage ≤ 500 V in the case of permanently installed cables and cords and may be operated with nominal voltages ≤ 250 V in the case of non-permanently installed cables and cords.

9.2.2 Preferred nominal voltages

The following nominal voltages should be used for preference:

a) AC voltage: 24 V, 48 V, 110 V, 230 V;

b) DC voltage: 24 V, 48 V, 60 V, 220 V.

See 4.3 with regard to voltage tolerances.

9.3 Connection to the protective conductor

With a supply from control supply transformers, converters or batteries, the auxiliary circuits shall be connected to the protective conductor.

If it is not earthed, then there shall be an earth monitoring system, and the system shall be designed that two earth faults do not result in a hazardous fault. See also note of 9.1.1.

Control circuits shall be connected to the protective conductor if an unplanned shutdown, caused by a second unplanned connection to earth is acceptable.

A detachable connection to the protective conductor shall be provided at the control-power transformer or in the vicinity of converters or batteries.

9.4 Overcurrent protection of auxiliary circuits

9.4.1 Rating of overcurrent protective devices

Conductors and contact elements in auxiliary circuits shall be protected against overcurrent. The overcurrent protective devices shall be selected such that, in the event of a short circuit, they switch off the auxiliary

circuit automatically within one second. This does not apply for auxiliary circuits with current limiters connected to safety-related circuits, if the effectiveness of the safety-related system is not impaired by the initial fault (see Figure 10), or contact elements are protected against permanent welding.

All impedance in the auxiliary circuit shall be taken into account in the rating of the overcurrent protection (e.g. control supply transformers, fuses, conductors).

When selecting the overcurrent protective devices, the manufacturer's data concerning the permissible overcurrent of the contact elements used in the auxiliary circuits shall also be taken into account.

9.4.2 Overcurrent protection of auxiliary circuits connected to the protective conductor

Overcurrent protection of an auxiliary circuit shall not be connected into the conductor which is connected to the protective conductor.

9.4.3 Overcurrent protection of auxiliary circuit with the middle conductor connected to the protective conductor

Auxiliary circuits with an earthed centre tapping of the auxiliary power source connected to the protective conductor shall be protected against overcurrents at both line conductors.

9.4.4 Overcurrent protection of auxiliary circuits with no electrical connection to the protective conductor

Auxiliary circuits with no electrical connection to the protective conductor shall be protected against overcurrents in the conductor in which the contact elements are located (see also 9.5 c).

On ships, in the case of auxiliary circuits with no connection to the protective conductor, both conductors shall be protected against overcurrents.

9.4.5 Overcurrent protection of control system supply transformers

Overcurrent protection on the secondary side of control system supply transformers is not required if an equivalent overcurrent protection is provided by protective devices on the primary side.

9.4.6 Rating and setting of overcurrent protection

The ratings and setting of overcurrent protection devices shall be stated at the mounting location and in the circuit documentation.

9.5 Measures to prevent danger from short circuits to exposed conductive parts or earth

Short circuits to exposed conductive parts or earth shall cause no danger to persons or damage to the plant.

In order to meet this requirement, the following measures are necessary (individually or combined):

a) all the electrical actuating elements, e.g. contactor coils, shall be connected to a common conductor. In control circuits connected to the protective conductor, this common conductor shall be connected to the protective conductor;

b) in control circuits connected to the protective conductor, regardless of the magnitude of voltage, non-live metal parts of the equipment where a short circuit to an exposed conductive part or earth can occur shall be connected to the protective conductor by means of a conductor. This conductor shall be colour coded green/yellow if structural parts as specified in 6.2 are not used. In the event of a short circuit to an exposed conductive part or earth, the control circuit shall switch off automatically within one second;

c) this does not apply to control circuits if fault assessment in accordance with Figure 10 or Figure 11 results in termination (end of assessment);

d) in control circuits not connected to the protective conductor, regardless of the magnitude of voltage, an insulation monitoring device shall be present to signal any reduction beyond the permissible minimum value of insulation resistance. The internal resistance of the insulation monitoring device shall be sufficiently high to prevent any current exceeding 0,7 times the release value of the actuating element from flowing in the case of a possible cascade connection of the insulation monitoring device and actuating element in the event of a short circuit to an exposed conductive part or earth. All non-live metal parts shall be conductively connected to each other and to the earthing point of the insulation monitoring device.

9.6 Influence of capacitance and leakage resistance

Measures shall be taken to ensure that, in a fault-free control network, the sum of the currents which can still flow between conductors via the actuating element as the result of capacitance and leakage resistance after switching off does not exceed 0,7 times the release value of the actuating element with the smallest release value.

Sum of leakage currents:

$$(I_c + I_A) < 0,7 I_{Rmin}$$

where

I_c capacitive current between the conductor cores and between the latter and earth;

I_A leakage current (to earth);

$I_{R\,min}$ smallest release value of current for the actuating element concerned.

10 Additional requirements for the application of a safety-related system

10.1 General safety requirements

NOTE This clause considers that a furnace comprises ancillary equipment, heated systems, control system and safety related system (see Figure 1).

10.1.1 Safety lifecycle requirements for a safety-related system

In order to deal in a systematic manner with all the activities necessary to achieve the required safety integrity levels for the safety-related system, this standard adopts a safety lifecycle model (see Figure 8) as the technical framework.

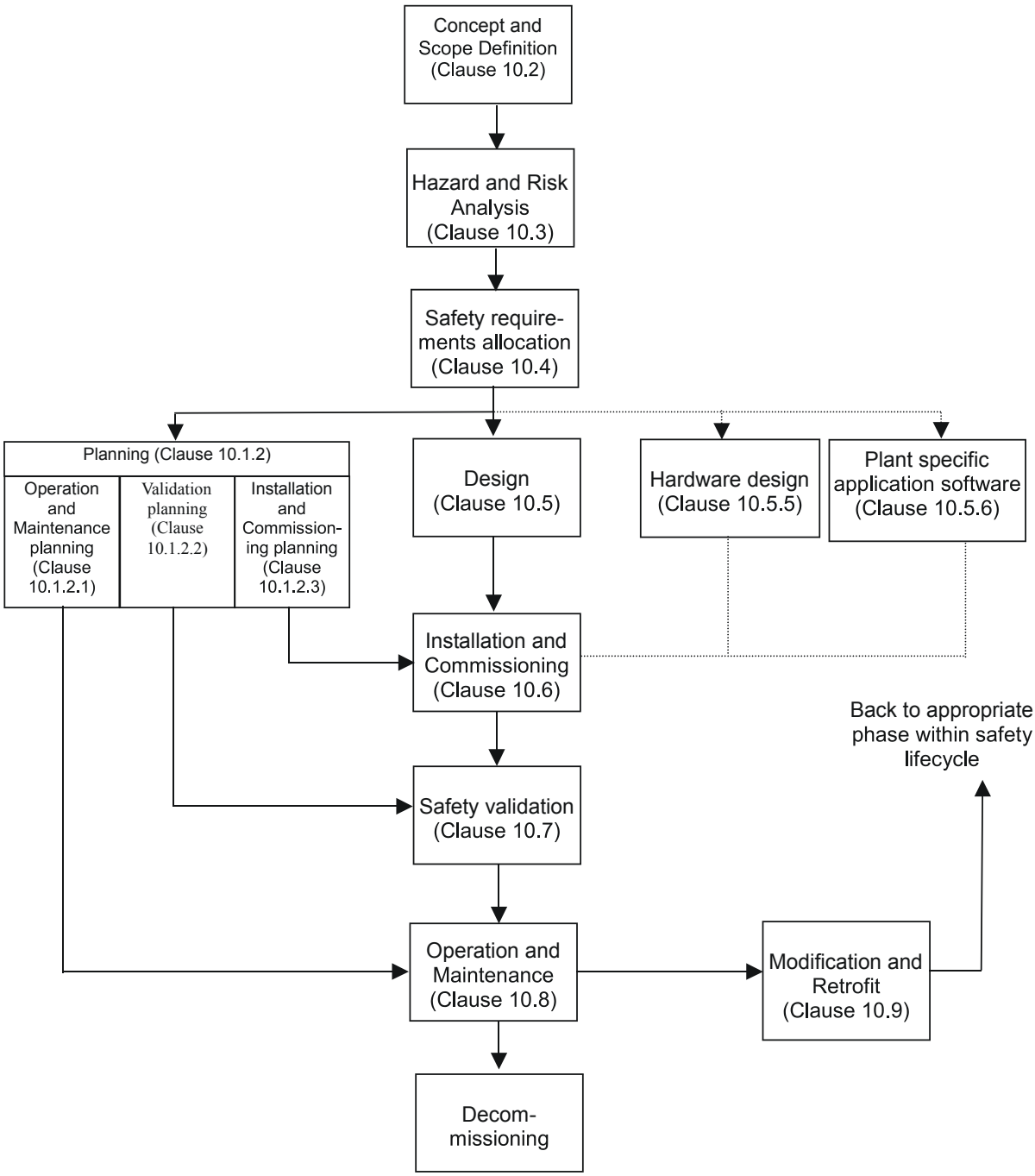


Figure 8 – Safety lifecycle model for application, design and installation of a safety-related system (Clause 10)

Activities relating to the management of functional safety and functional safety assessment are not shown on the safety lifecycle model. This has been done in order to reduce the complexity of the safety lifecycle figure and these activities, where required, will need to be applied in the relevant phases during the application, design and installation of a safety-related system using the guidance provided in Annex B (informative).

The objective of each safety lifecycle phase is as follows:

Concept and scope definition (10.2)	–	to develop a level of understanding of the furnace with its ancillary equipment, heated systems, control system and safety related system so that other lifecycle activities can be undertaken.
Hazard and risk analysis (10.3)	–	to determine the hazards and hazardous events of the furnace with its ancillary equipment and its control systems (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse
		NOTE Foreseeable misuse may be covered by organisational measures.
Safety requirements allocation (10.4)	–	to allocate the safety functions contained in the specification for the overall safety requirements (i.e. the safety functions requirements and the safety integrity requirements) to the furnace safety-related system.
Planning (10.1.2)	–	to develop plans to facilitate operation and maintenance, installation and commissioning, and validation of the furnace safety-related system in order to ensure that the required functional safety is achieved.
Design (10.5)	–	to create a safety related system which conforms to the safety requirements specification whereby each safety function can satisfy its safety requirements allocation.
Installation and commissioning (10.6)	–	to install and commission the safety-related system in accordance with the installation and commissioning plan.
Safety validation (10.7)	–	to validate that the safety-related system meets the specification for the overall safety requirements in terms of both safety functions and safety integrity requirements taking into account the safety requirements allocation.
Operation and maintenance (10.8)	–	to operate and maintain the safety-related system in order that the required functional safety is maintained.
Modification and retrofit (10.9)	–	to ensure that the functional safety for the safety-related system is appropriate, both during and after modification and retrofit activities have taken place.
Decommissioning	–	to ensure that the functional safety for the safety-related system is appropriate until the end of operation of the furnace with its ancillary equipment.

10.1.2 Planning

10.1.2.1 General

Plans should be developed in order to facilitate the requirements for functional safety provided by the furnace safety-related system at three distinct stages during its implementation and use in accordance with Figure 8.

10.1.2.2 Operation and maintenance planning

A plan shall be prepared which specifies the following:

a) the routine actions which need to be carried out to maintain the required functional safety of the safety-related system;

b) the actions and constraints that are necessary (for example during start-up, normal operation, routine testing, foreseeable disturbances, faults and shutdown) to prevent an unsafe state, to reduce the demands on the furnace safety-related system or reduce the consequences of the hazardous events;

NOTE 1 The following constraints, conditions and actions are relevant to the safety-related system implemented:

– constraints on the furnace operation during a fault or failure of the safety-related system;

– constraints on the furnace operation during maintenance of the safety-related system;

– when constraints on the furnace operation may be removed;

– the procedures for returning to normal operation;

– the procedures for confirming that normal operation has been achieved;

– the circumstances under which the safety-related system safety functions may be by-passed for start-up, for special operation or for testing;

– the procedures to be followed before, during and after by-passing safety-related system safety functions, including permit to work procedures and authority levels.

c) the documentation which needs to be maintained showing results of functional safety audits and tests;

d) the documentation which needs to be maintained on hazardous incidents and all incidents with the potential to create a hazardous event;

e) the scope of the maintenance activities (as distinct from the modification activities);

f) the actions to be taken in the event of hazards occurring;

g) the contents of the chronological documentation of operation and maintenance activities (see 10.8).

A safety-related system may have some failure modes which can be revealed only by testing during routine maintenance. In such cases, if testing is not carried out at sufficient frequency, the required safety integrity of a safety-related system will not be achieved. Where testing is carried out online, it may be necessary to disable the safety-related system on a temporary basis. This should be considered only if the probability of a demand occurring during this time is remote. Where this cannot be ensured, it may be necessary to install additional sensors and actuating elements to maintain the required functional safety during testing.

NOTE 2 This clause also applies to suppliers of software who are required to provide information and procedures with the software product that will allow the user to ensure the required functional safety during the operation and maintenance of a safety-related system. This includes preparing procedures for any software modification that could come about as a consequence of an operational or maintenance requirement.

h) The routine maintenance activities which are carried out to detect unrevealed faults should be determined by a systematic analysis.

NOTE 3 If unrevealed faults are not detected, it may

– lead to a failure of the safety-related system to operate on demand,

– in the case of non-safety-related systems, lead to demands on the safety-related system.

i) The plan for maintaining the safety-related system shall be agreed upon with those responsible for the future operation and maintenance of the safety-related system and the non-safety-related systems that have the potential to place demands on the safety-related system.

10.1.2.3 Validation planning

A plan shall be developed which shall include the following:

a) details of when the validation shall take place;

b) details of those who shall carry out the validation;

c) specification of the relevant modes of the furnace operation with their relationship to the safety-related system, including where applicable:

- preparation for use including setting and adjustment;
- start up;
- teach;
- automatic;
- manual;
- semi-automatic;
- steady-state of operation;
- re-setting;
- shut down;
- maintenance;
- reasonably foreseeable abnormal conditions;

d) specification of the safety-related system safety functions which need to be validated for each mode of furnace operation before commissioning commences;

e) the technical strategy for the validation (for example, analytical methods, statistical tests, etc.);

f) the measures, techniques and procedures that shall be used for confirming that the allocation of safety functions has been carried out correctly, this shall include confirmation that each safety-related system safety function conforms

- with the specification for the overall safety functions requirements, and
- to the specification for the overall safety integrity requirements;

g) the required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment);

h) the pass and fail criteria;

i) the policies and procedures for evaluating the results of the validation, particularly failures.

In planning the validation activities, account should be taken of the work planned for safety validation of both hardware and software elements of the furnace safety-related system as required by 10.5. It is important to ensure that the interactions between all risk reduction measures are considered and all safety functions have been achieved.

The information from a) to i) above shall be documented and shall constitute the plan for the safety validation of the furnace safety-related system.

10.1.2.4 Installation and commissioning planning

A plan for the installation and commissioning of the furnace safety-related system shall be developed, specifying the following:

- the installation schedule;
- those responsible for different parts of the installation;

– the procedures for the installation;

– the sequence in which the various elements are integrated;

– the criteria for declaring all or parts of the safety-related system ready for installation and for declaring installation activities complete;

– procedures for the resolution of failures and incompatibilities;

– the commissioning schedule;

– those responsible for different parts of the commissioning;

– the procedures for the commissioning;

– the relationships to the different steps in the installation;

– the relationships to the validation.

The overall installation and commissioning planning activities shall be documented so that the above activities take place in a controlled manner, to ensure that the required level of functional safety is achieved.

10.2 Concept and scope definition

The requirement of this clause is to develop a level of understanding of the furnace and its environment (physical, legislative etc.) to enable the other safety lifecycle activities to be satisfactorily carried out. This necessarily involves determination of the full extent of the furnace installation, complete with ancillary equipment, heated systems, control system and safety related system, so that the scope of a hazard and risk analysis (for example, combustion hazards, environmental hazards, etc.) can be specified. This includes non-electrical sub-systems which are electrical controlled, directly or indirectly.

This concept can be part of application standards (e.g. EN 12952, EN 12953). In this case, the standards specify the requirements to the control system and safety related system.

In particular, consideration should be given to determining the following:

a) a thorough familiarity shall be acquired of the furnace, its required control functions and its physical environment;

b) the likely sources of hazards shall be determined;

c) information about the determined hazards shall be obtained (explosive conditions, corrosiveness, reactivity, flammability etc.);

d) information about the current safety regulations (national and international) shall be obtained;

e) the physical equipment (including the furnace complete with ancillary equipment, heated systems, control system and safety related system) to be included in the scope of the hazard and risk analysis shall be specified;

f) the external events to be taken into account in the hazard and risk analysis shall be specified;

g) the sub-systems which are associated with the hazards shall be specified;

h) the type of accident-initiating events that need to be considered (for example, component failures, procedural faults, human error, dependent failure mechanisms which can cause accident sequences to occur) shall be specified.

The information and results acquired in a) to h) shall be documented.

10.3 Hazard and risk analysis

For each furnace, comprising ancillary equipment, heated systems, control system and safety related system, a hazard and risk analysis (see examples of potential hazards in 4.1) shall be undertaken using information from the concept and scope definition phase (see 10.2). For boiler installations based on EN 12952 and EN 12953, the hazard analysis for the furnace based on these standards is included in the parts EN 12952-7; EN 12952-8; EN 12952-9; EN 12952-16, EN 12953-6; EN 12953-7; EN 12953-12

This analysis shall be performed by a team of persons who are competent to discharge responsibilities associated with this lifecycle activity. The training, technical knowledge, experience and qualifications of those involved should be relevant to the particular application (e.g. process technology, process safety, furnace operations, process control, safety-related systems specialist, etc.).

In practice it is recommended that a facilitator be appointed to guide the team in a systematic manner through the hazard and risk analysis leading to the allocation of safety integrity levels for each safety function performed by the safety-related system. The facilitator should be responsible for documenting the outcome of the hazard and risk analysis and safety requirements allocation (see 10.4) phases in collaboration with representatives of conformity assessment establishments, as necessary.

The basic requirements and approaches of different methods of the risk analysis are included in EN 61508-5. A quantitative approach to the hazard and risk analysis based on EN 61508-5 may be used as an alternative to the qualitative method, described here.

NOTE The appropriateness of the techniques, and the extent to which the techniques will need to be applied, will depend on a number of factors, including:

– the specific hazards and the consequences,

– the legal and safety regulatory requirements,

– the risks associated with the furnace operation, and

– the availability of accurate data upon which the hazard and risk analysis is to be based.

For each furnace and its ancillary equipment the hazard and risk analysis shall consider the following parameters:

– each determined hazardous event and the components that contribute to it;

– the consequences and likelihood of the event sequences with which each hazardous event is associated;

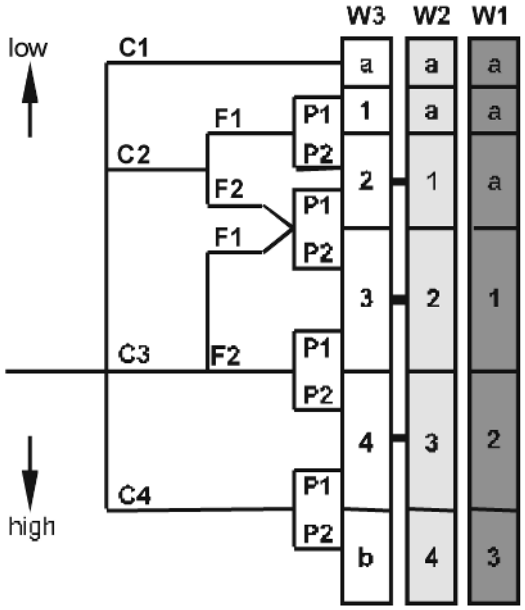
– the necessary risk reduction for each hazardous event;

– the measures taken to reduce or remove hazards and risks;

– the assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates – any credit taken for operational constraints or human intervention shall be detailed;

and the resulting requirements in terms of the safety-related system.

Figure 9 shows the relationship between the risk parameters and safety integrity level allocation for a furnace safety-related system in the form of a risk graph. Examples of risk analysis see Annex D.



Required safety integrity level:
a Standard control systems;
1,2,3,4 Safety integrity levels;
b A single safety-related system is not sufficient.
For ratings of requirements for safety-related systems see Table 1.
Risk parameters:
– Consequences of the hazardous event;
C1 Minor injury;
C2 Serious permanent injury to one or more persons or death to one person;
C3 Death to several people;
C4 Very many people killed.
– Frequency and exposure time to hazard;
F1 Rare to more often;
F2 Frequent to permanent.
– Possibility of avoiding the hazardous event;
P1 Possible under certain conditions;
P2 Almost impossible.
– Probability of unwanted occurrence;
W1 Very slight probability;
W2 Slight probability;
W3 Relatively high probability.

Figure 9 – Rating of safety integrity levels for furnaces

10.4 Safety requirements allocation

The safety requirements allocation shall identify and specify:

– the required safety functions in order to achieve functional safety;

– the system reaction in the case of faults should be defined. This includes sensors and actuating elements with the interface to the process.

– whether the safety function is applicable to a protection system which is operated in demand mode or continuous operation;

– throughput and response time performance;

– safety related system and operator emergency stop device;

– any other safety-relevant information which may have an influence on the safety device design;

– all interfaces between the safety-related system and any other systems (either directly associated within, or outside the furnace);

– all relevant modes of operation of the furnace and its associated equipment*:*

NOTE Additional safety functions may be required for particular modes of operation (e.g. setting, adjustment or maintenance) to enable these operations to be carried out safely.

– all required modes of behaviour of the safety-related system. In particular, failure behaviour and the required response of the safety devices shall be detailed;

– all environmental conditions which are necessary to achieve function safety;

– the procedures for starting up and restarting the safety related system;

– those requirements necessary to enable monitoring of the safety related system hardware to be undertaken;

– facilities for function testing of the safety functions;

– the Safety Integrity Level for each safety function;

– the requirements for function testing (proof testing).

Annex D shows examples how risk parameters for particular furnaces or parts thereof may be estimated and the resulting safety integrity levels.

When estimating the probability of the unwanted occurrence field, it should be recognized that non-safety-related control and monitoring systems, which are reliable and functioning independently from and do not interact with the safety-related system, may result in a reduced probability of the unwanted occurrence (compared to a plant without such equipment). It may therefore be appropriate to allocate a lower than necessary safety integrity level of the safety related system.

For additional information regarding the credit that can be claimed from standard control systems (e.g. a furnace control system), please refer to EN 61508-1:2010, 7.5 (overall safety requirements).

10.5 Design

10.5.1 General requirements

Techniques for avoiding (preventing the introduction of) systematic faults during design and development and design features (e.g. self-checking, redundancy) in the safety related system for controlling both random and systematic faults during operation shall be applied.

For the design the principals of Figure 10 shall be used. For application in accordance with this standard Route 2H in accordance with EN 61508-2 shall not be used. If the safety related system consists of a combination of subsystems or devices in accordance with EN 61508 and type-tested subsystems or devices not provided with reliability parameters, it shall follow from the numerical evidence that the safety integrity of the safety related system complies with the required safety integrity level.

NOTE 1 For the safety related system a distribution of the probability of failure is assumed as follows: 35 % (sensor subsystem), 15 % (logic subsystem), 50 % (actuating element subsystem).

It shall follow from the numerical evidence that the allowed probability of failure is exhausted by use of the components provided with reliability parameters not exceeding the above mentioned percentage.

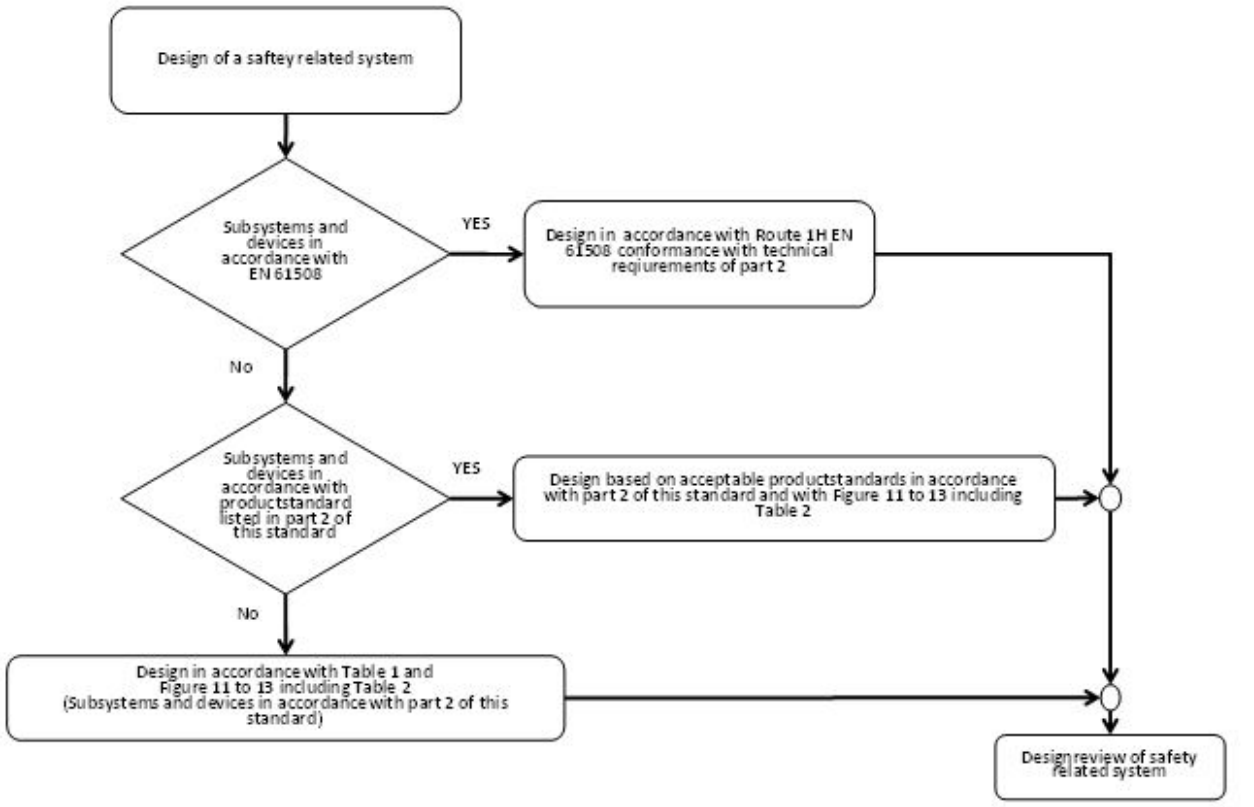


Figure 10 – Choice of design principals

NOTE 2 Based on the application of Figure 11, Figure 12 and Figure 13, a hazardous situation caused by a single fault of the safety related system can be excluded.

10.5.2 Design of the safety-related system

For the design of the safety-related system, the fault analysis following the procedure in the fault charts Figure 11 or Figure 12 and Figure 13 depending on the technology has to be employed. This should include considering the following:

– monitors, limiters, measuring devices and limit monitors which shall trigger the establishing of the safe status of the plant (e.g. interruption of the fuel flow) when limits are exceeded;

– safety related system reacting to these input signals (see Figure 1);

– actuating elements which establish the safe status (e.g. fuel trip valves) as well as their switching devices (e.g. relays, contactors and breakers).

The design and type-approval of safety devices is subject to Part 2 of this standard. The following requirements (including Hardware and Plant specific application software) cover the application of such type – approved equipment (according to Part 2 of this standard or other relevant safety standards) in a plant-specific safety-related system in combination with cabling, other non-safety-related equipment, etc.

For the design of the safety related system subsystems or devices in accordance with part 2 of this standard shall be used. Excluded are switching units fulfilling the requirements of 10.5.5.3 and 10.5.5.4.

EN 50156-1:2015 (E)

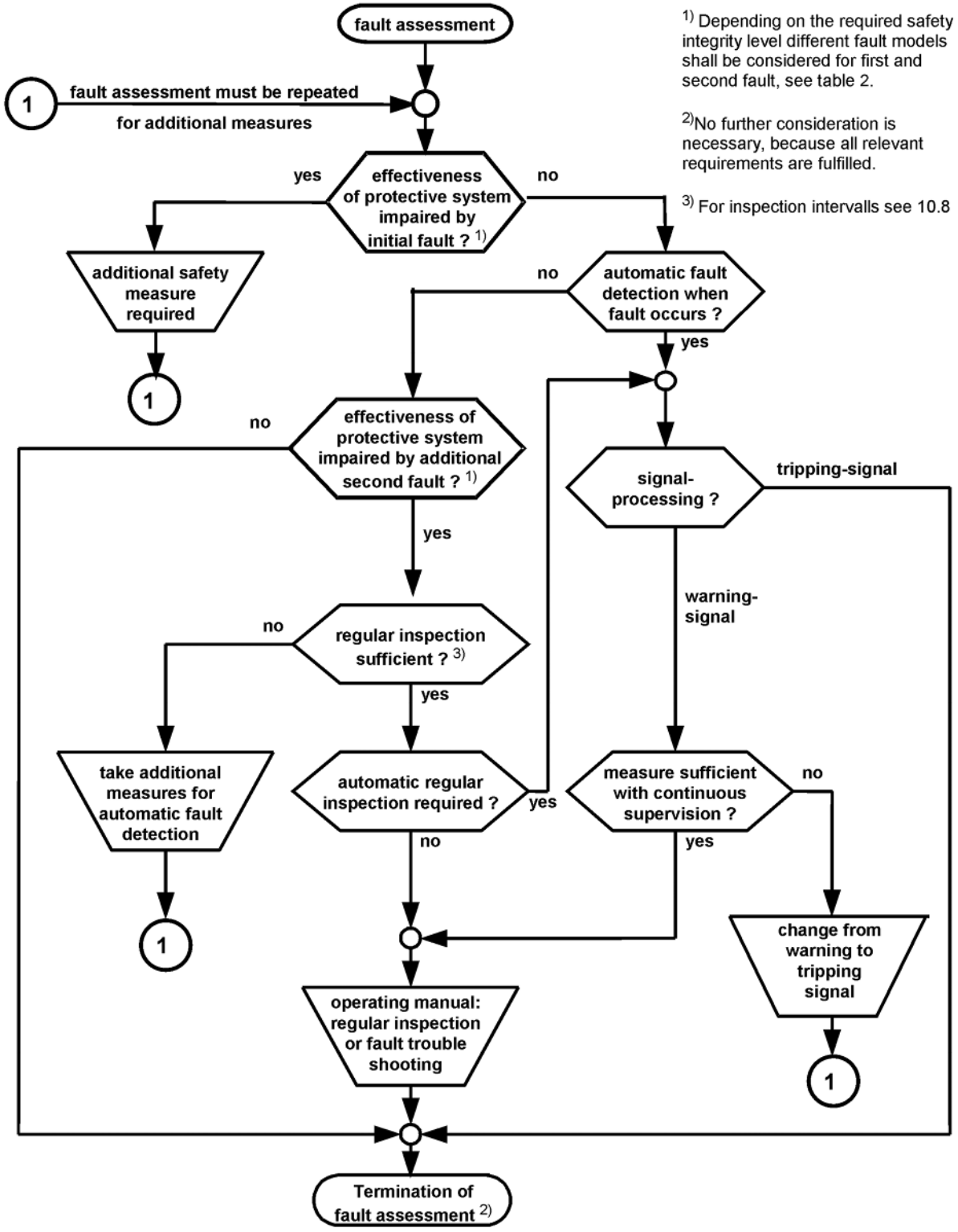


Figure 11 – Fault assessment for the hard-wired section of a safety-related system

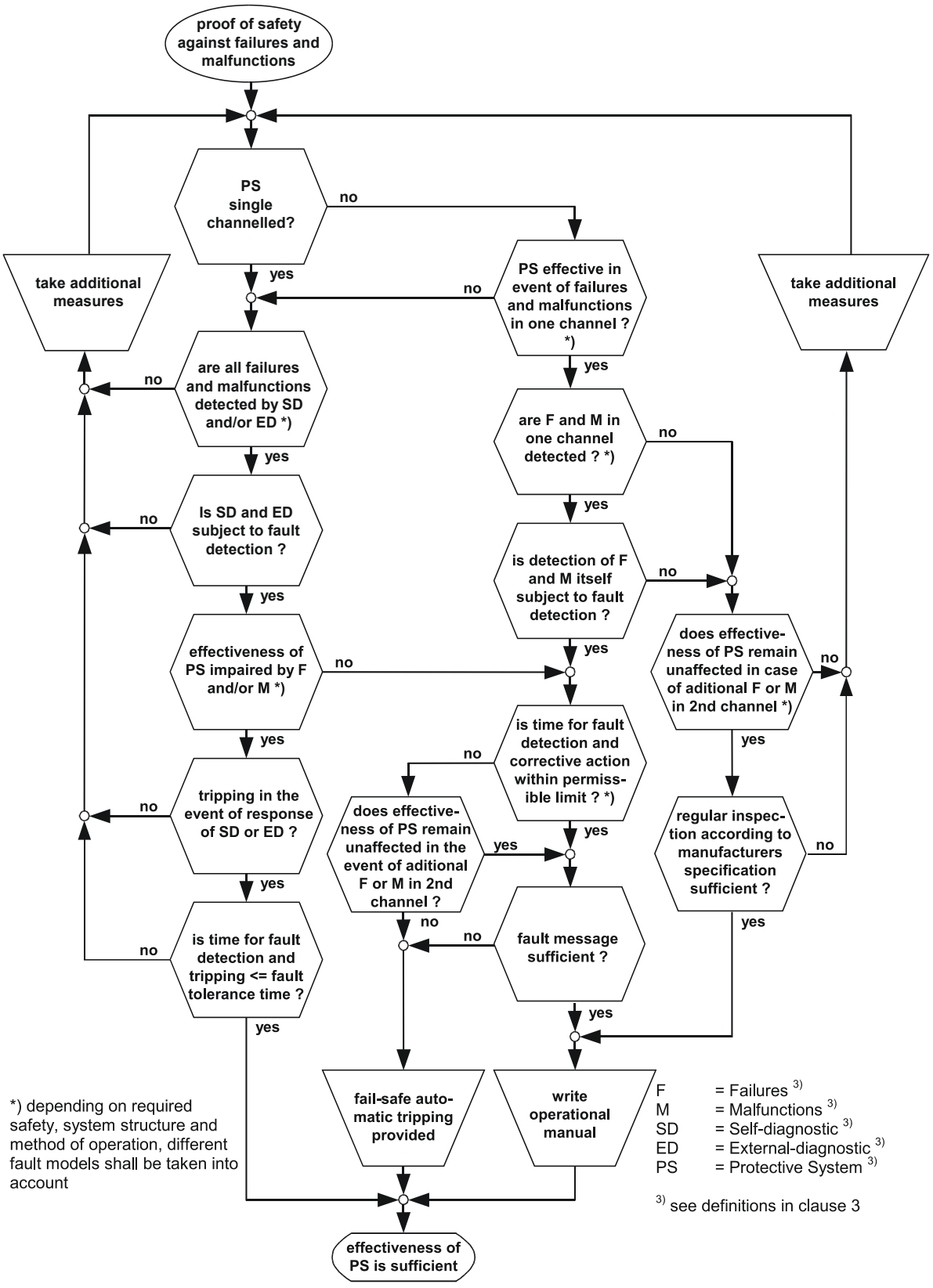


Figure 12 – Proof of safety against failures and malfunctions of the programmable safety device of the safety-related system

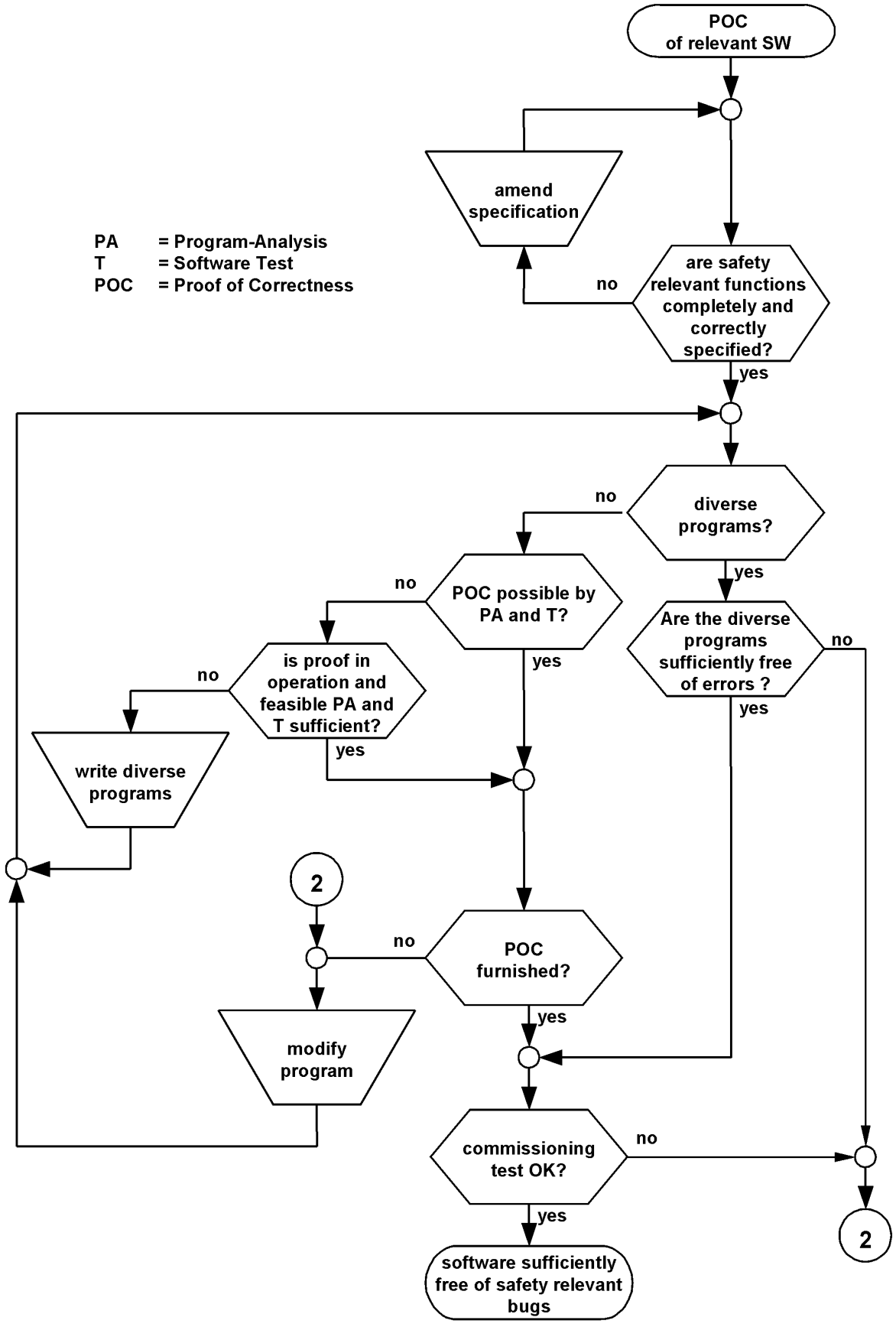


Figure 13 – Proof of safety of software

Table 1 – Consideration of different field equipment (sensors and actuating elements) configurations if subsystems or devices are used based on product standards without data in accordance with EN 61508 or only based on the fault assessment in accordance on the Figures 11, 12 or 13

Safety integrity level	Configuration a, c	Interval of operation between two functional tests	Diagnostic coverage
1	1oo1	< = 1 month	None
	1oo1	< = 6 months	Simple
	1oo1	< = 1 year	Medium
	2oo2	< = 1 month	None
	2oo2	< = 6 months	Simple
	2oo2	< = 1 year	Medium
2	1oo1	< = 1 month	Medium
	1oo1	< = 1 year	high-grade
	2oo2	< = 1 month	Medium
	2oo2	< = 1 year	high-grade
	1oo2	< = 6 months	None
	1oo2	< = 1 year	Medium
	2oo3	< = 1 month	None
	2oo3	< = 1 year	Simple
3			
	1oo2	< = 1 month	none[b] (only type A[)e]
	1oo2	< = 6 months	simple[b]
	1oo2	< = 1 year	medium[b]
	2oo3	< = 1 month	none[b] (only type A)[e]
	2oo3	< = 6 months	simple[b]
	2oo3	< = 1 year	medium[b]

[a] Configuration of field equipment (sensors and/or actuating elements).

[b] Permissible if numerical fault analysis has been carried out to prove reliability; otherwise high diagnostic coverage of faults is necessary.

[c] The different channels of the field equipment shall work independently of each other.

[d] Medium or high-grade diagnostic coverage may only be considered if the analogue outputs of the transmitters are monitored continuously. (see EN 61508–2 Annex A)

[e] Type A according to EN 61508–2.

Configuration	Description
1oo1	single channel configuration.
2oo2	dual channel operation, both shall respond to actuate tripping.
1oo2	dual channel operation, tripping is actuated if one responds.
2oo3	2 out of 3 configuration.

The safety-related system shall be designed such that:

a) faults which could impair the effectiveness of the safety-related system shall be avoided or

b) in the event of internal faults or the occurrence of external influences in or at the safety device

   1) its effectiveness remains unaffected, or

   2) the plant remains in a safe condition, or it is brought to a safe condition (by fault control techniques).

The simultaneous occurrence of two independent faults in different components need not be taken into account. The addition of a second fault to an undetected initial fault shall, however, be taken into account, in accordance with Figure 11 or Figure 12.

The configuration of the safety-related system shall be chosen to meet the required safety integrity level and the maximum operational intervals between two functional tests shall be selected to ensure that the required safety integrity level is achieved (see Table 1).

The reaction to a fault which negatively affects the effectiveness of the safety-related system shall be as described in the following:

– a single channel safety-related system shall trip into a safe state;

– a multiple channel safety-related system can trip into a degraded mode. The time limit for the degraded mode of operation depends on the requirements of the plant (operation with or without supervision) and the result of the calculation of the second fault occurrence time according to the probability of failure on demand (EN 61508-1, EN 61508-2).

– for the safety-related inputs and outputs of the safety-related system the tripping of the affected parts of the application could be sufficient.

10.5.3 Measures to avoid faults

During development, organisational and design precautions shall be taken to avoid faults, for example:

a) stipulation of a project-specific production sequence plan, for example, broken down into

   1) specifications,

   2) design (schematic, circuit diagram, parts lists, hardware design),

   3) prototype,

   4) test plan.

b) segregation of safety-related and non-safety-related subsystems referred to the particular unit under consideration;

c) conducting a fault possibility and influence analysis;

d) application of computer-aided design systems;

e) overdimensioning of components.

Particular attention has to be paid to fault avoidance precautions in the case of application of specific integrated circuits (see EN 61508-2).

10.5.4 Consideration of times

The consideration of fault tolerance time and safety time concerning furnaces is shown in Figure 14.

The sum of safety time and the closing time of the shut off valve or the final element shall be less than the fault tolerance time of the relevant process function.

The timing requirements for a particular furnace are determined either by design parameters specific to the application or can be determined by specific testing.

NOTE The safety time following flame interrupt is usually between one and three seconds.

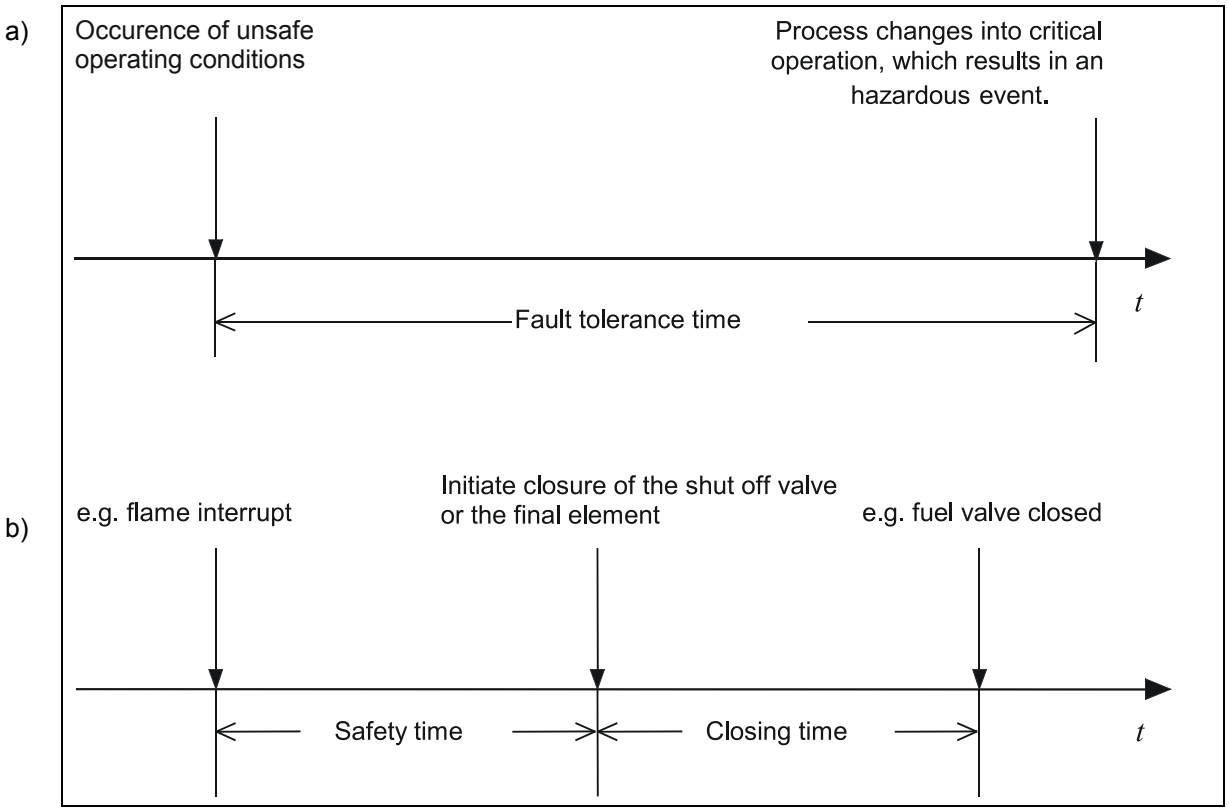


Figure 14 – Consideration of fault tolerance time and safety time for furnaces

10.5.5 Hardware design

10.5.5.1 General requirements of the hardware

a) The system description shall be readily comprehensible and logically structured, and it shall clearly depict the safety philosophy and the safety functions.

b) Required function, reaction in the event of a fault, interfaces (software, hardware) and the permissible environmental influences of a functional unit within the system shall be unambiguously specified.

10.5.5.2 Hard-wired section of the safety-related system

The hard-wired section of the safety-related system shall be constructed such that fault assessment according to Figure 11 results in termination. This stipulation applies for safety integrity levels 1, 2 and 3.

Fault assessment for the safety related system according Figure 11 shall consider failure of auxiliary power and break of connecting lines. If plant components affected by such failures achieve a safe status (e.g. closed-circuit operation in binary circuits), a single-channel design of the relevant parts may be sufficient apart from the following measures.

If this cannot be assumed (e.g. open-circuit operation of binary circuits) a second independent trip channel shall be provided in order to achieve the effectiveness of the safety-related system (including all pneumatic, hydraulic and mechanical actuating elements) for this function.

In the case of non-solid state circuits, at least two monitored disconnecting devices, i.e. contactor or relay, shall be provided to obtain safety shutdown of the entire fuel supply to the furnace.

For furnaces which operate continuously where regular inspections at sufficiently short intervals (calculated according to EN 61508-1, EN 61508-2, EN 61508-6 and based on architecture, HTF, SFF, e.g. half a year, one year) in accordance with Figure 11 may not be performed, disconnecting devices (relays) with diverse functionality or hardware diversity shall be provided to shut down the entire fuel supply.

Reed relays shall not be used for any safety-related functions, unless remanence is covered by continuous testing.

NOTE 1 Table 1 contains information regarding the maximum interval between functional tests depending on the required safety integrity level and the configuration of the safety-related system for continuous operation.

NOTE 2 Diverse functionality is achieved by closed-circuit arrangement and open-circuit arrangement, for example, as in Figure 16. Hardware diversity is achieved by different types of construction of electro-mechanical switching devices, for example, i.e. if switching devices of different construction or design are used (Figure 15).

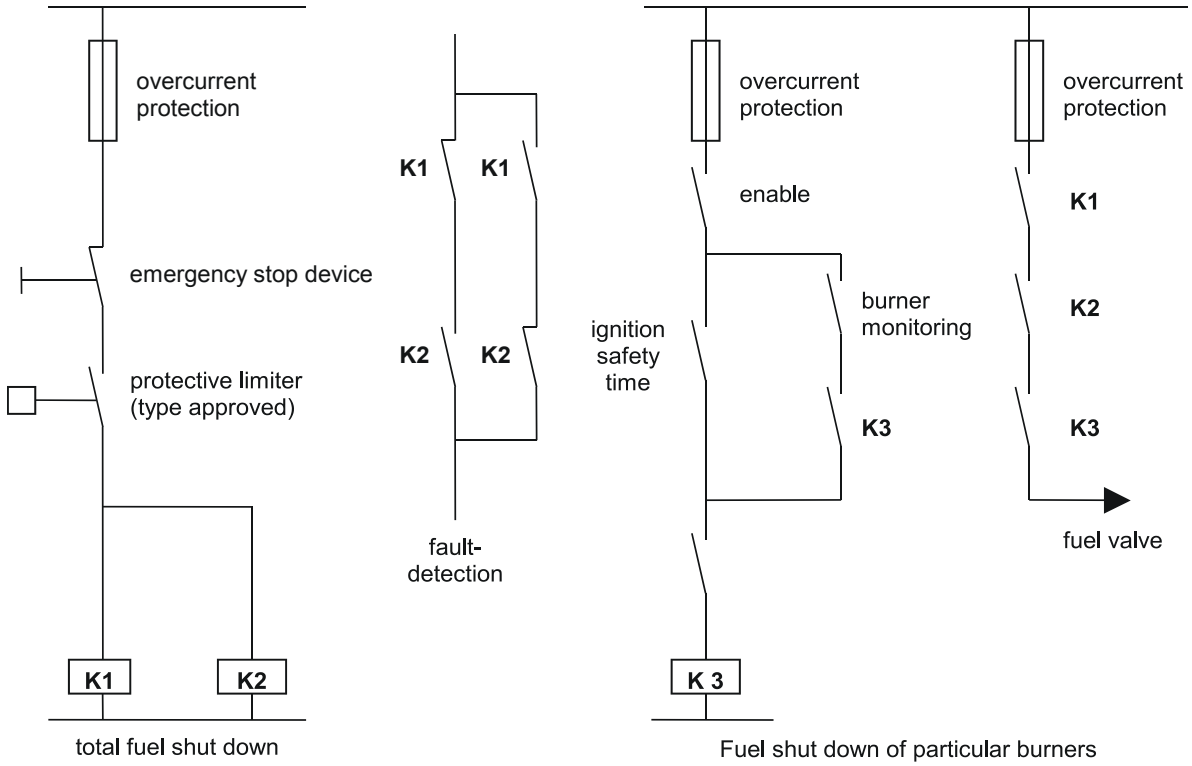


Figure 15 – Examples for wiring of fuel shut down with hardware diversity of the disconnecting devices

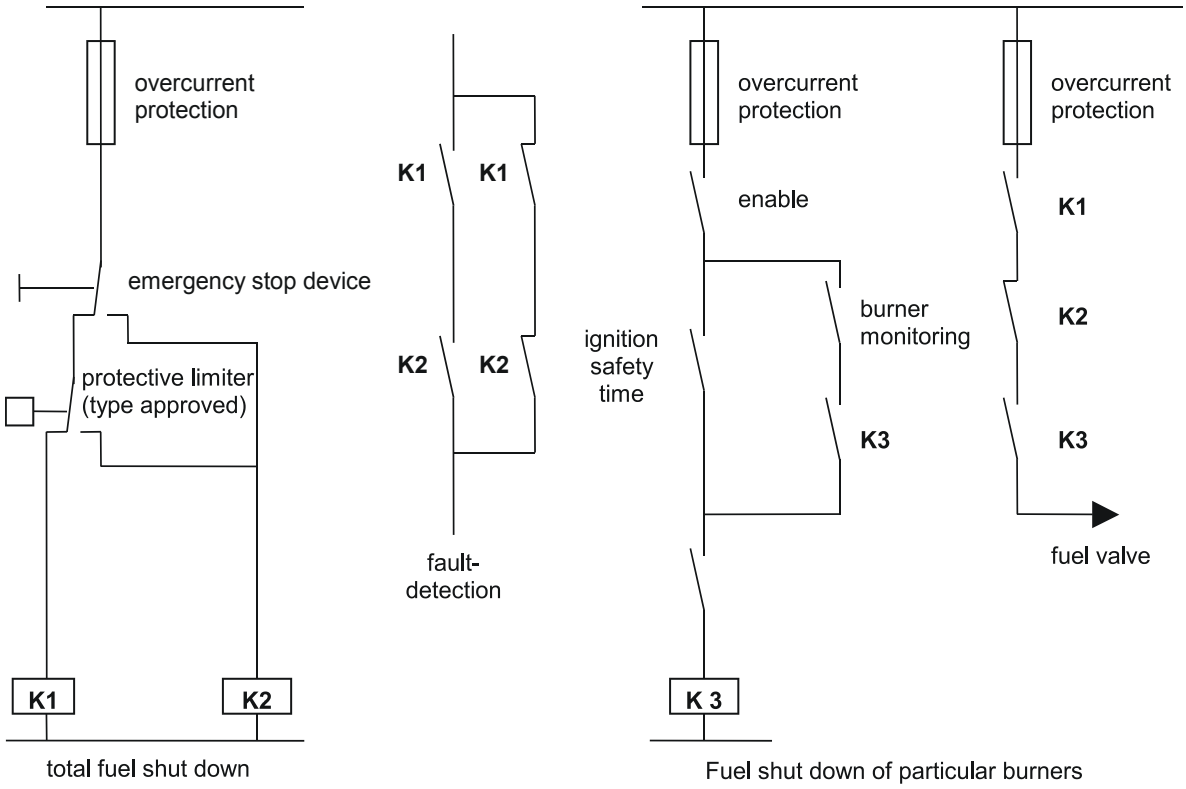


Figure 16 – Example for wiring of fuel shut down with diverse functionality of the disconnecting devices

10.5.5.3 Fault exclusions

10.5.5.3.1 General

With fault assessment according to Figure 11 and Figure 12 it is assumed that certain faults do not occur. Such assumptions are justified by describing the failure mechanism as well as by stating the conditions relating to design, construction, environment etc. for the conductors, components and equipment. Table 2 shows possible fault exclusions depending on the required safety integrity level.

Table 2 – Allocation of fault exclusions to safety integrity levels

Fault exclusion	Safety integrity level 1 or 2	Safety integrity level 3
Conductor to conductor short circuit	+	+[a]
Short circuit in wound film resistors	+	+[a]
Short circuit in wire-wound resistors	+	+[a]
Non-opening of contact elements due to permanent welding	+[a]	o
Mechanical failure of switching devices	+[a]	o
Inter-winding short circuits in transformers	+[a]	+[a]
Transient voltages in switching devices like relays, contactors or auxiliary contacts between the contacts and between contact and coil	+[a]	+[a]
Short-circuiting of isolating distances in optocouplers	+[a]	+[a]
Break of spring in actuating element (valve)	+[b]	o
Mechanical failure of actuating element with sufficient reserve in actuating force	+[b]	o
Non-release of fail-to-safe solenoid valves	+[b]	o
Position switch with positive opening contacts	+[b]	o
Gas warning device with switching function	o	o
Key: + = permissible, o = not permissible		
[a] Fault exclusions see (10.5.5.3). [b] If devices are used according to 10.5.3.		

The following faults may be excluded without further justification:

10.5.5.3.2 Conductor-to-conductor short circuit

„Conductor-to-conductor short circuit“ fault.

a) For cables and conductors as specified in Clause 12;

b) If the clearances between live parts are designed according to overvoltage category III and pollution degree 3 and the creepage distances are designed according to pollution degree 3 but at least for the nominal voltage 63 V as specified in EN 60664-1;

c) If components are encapsulated so that they are moisture-resistant or if they are hermetically sealed and they withstand a test as specified in Part 2 of this standard;

d) If printed conductors (tracks) are varnished so that they are resistant to aging in accordance with the distances between the printed conductors are equivalent to at least the values specified in EN 60664-1:2007, Table 4 for pollution degree 1 but at least for a nominal voltage of 32 V (minimum creepage distance 0,14 mm).

10.5.5.3.3 Short circuit in wound film resistors

„Short circuit in wound film resistors“ fault if the latter are used with a varnished or encapsulated resistive layer and axial terminations. The possibility of condensation shall be excluded during operation. The limits, e.g. voltage limit, power, shall not be exceeded even under unfavourable conditions.

10.5.5.3.4 Short circuit in wire-wound resistors

„Short circuit in wire-wound resistors“ fault if the winding is a single-layer winding and it is secured by means of a glaze or embedding in sealing compound.

10.5.5.3.5 Non-opening of contact elements due to permanent welding

„Non-opening of contact elements due to permanent welding“ fault in the case of contactors, relays or auxiliary switches if they are protected against the effects of short circuits by an appropriate overcurrent protective or current limiting device. In rating of the overcurrent protective device, the nominal current of the overcurrent protective device stated by the switching device manufacturer is to be multiplied by a safety factor of 0,6. Fault exclusion is also permissible if the prospective short-circuit current is less than the nominal current for the contact element concerned. Where contact elements are connected in series, the contact element with the lowest overcurrent strength shall be the deciding factor.

This fault exclusion is not applicable for reed contacts. The fault exclusion also is not applicable for applications requiring safety integrity level 3 (see 10.5.5.2).

10.5.5.3.6 Mechanical failure of switching devices

„Mechanical failure of switching devices“ if they are still operative after at least 250 000 switching cycles under conditions similar to operating conditions. Contactors and relays shall additionally have a mechanical endurance of 3×10^6 switching cycles.

This fault exclusion is not applicable to reed contacts. The fault exclusion also is not applicable to applications requiring safety integrity level 3

NOTE The term „conditions similar to operating conditions“ covers chemical and climatic as well as electrical and mechanical stresses.

10.5.5.3.7 Faults in components for safe isolation

Faults in components which are provided for safe isolation of electrical circuits (e.g. power circuits and telecommunications circuits) in accordance with IEC 60536-2.

a) Inter-winding short circuits in transformers (e.g. primary-secondary):

   Transformers shall comply with the electrical and mechanical requirements of EN 61558-1. In deviation from EN 61558-1, for transformers with working voltages up to 200 V, insulation between windings and insulation against the core shall be designed for a test voltage of 2 kV r.m.s. at nominal voltages 200 V < U_B < 500 V for a test voltage of 3,75 kV r.m.s.. Transformers shall as a minimum be conditionally short-circuit proof. Shifting of windings, turns and connection lines shall be prevented, e.g. by vacuum impregnation or encapsulation.

b) Transient voltages of switching devices, like relays, contactors or auxiliary contacts between the contacts and between coil and contact.

   The insulation between the contacts or between coil and contact shall be designed for nominal voltages U_B up to 200 V for a test voltage of 2 kV r.m.s. at nominal voltages 200 V < U_B < 500 V for a test voltage of 3,75 kV r.m.s.. By means of special design features (e.g. caps, ribs, encapsulation, banding) at contacts and coils, safe isolation shall also be guaranteed in the event of faults, for example, spring breakage.

c) Short-circuiting of isolating distances in optocouplers:

   The clearances and creepage distances of the optocoupler in its installed position shall fulfil the relevant conditions of EN 60664-1:2007, Clauses 19 and 29.

10.5.5.4 Additional requirements for circuit breakers

The open-circuit arrangement may be used to operate latching breakers of motors with voltages up to 1 kV and outputs exceeding 150 kW as well as in the case of voltages exceeding 1 kV in electrical and closed electrical operating areas if the following conditions are met:

a) the extinguishing medium, the principle of stored energy in precharged closing springs for switching off and the trip of the circuit-breaker shall be so designed that there is no possibility of failure in the interrupt case. When a lockout device is triggered by extinguishing medium parameters dropping below their specified values, a serial-connected switch (e.g. the incoming-feeder circuit-breaker or a second branch-circuit breaker) shall be capable of independent switch-off. Switching off at the second breaker may not be delayed by more than 1 s. If it is not certain that faults can be immediately detected and cleared within the open-circuit/control circuit, a second tripping device with an independent control circuit shall be provided. The latter requirement is always applicable to safety integrity level 3;

NOTE If the drives to be tripped by the safety related system are supplied by a frequency converter, this requirement may be met adequately by immediate turn-off of the output of the frequency converter and tripping of the preceding breaker after the transient voltage has decayed after approximately two seconds.

b) contact members in main circuits, and the mechanism for opening the contact, and if necessary upstream overcurrent protection shall be designed such that a welding of the contacts may be excluded;

c) the breakers shall be maintained in accordance with the manufacturer's instructions and under consideration of the switching frequency so that their functionality is maintained;

d) the power supply for the control system shall be from a reliable power source, e.g. from a battery backed supply;

e) overcurrent protection devices in these control circuits shall have trip monitoring;

f) indications of failure of the control voltage, tripping of an overcurrent protective device and reductions below the required minimum value of insulation resistance in IT systems shall be transmitted to a permanently manned station. The transmission of a group monitored fault signal is adequate;

g) the disconnection of any control circuit plug-and-socket combination shall be automatically detected and an indication signal transmitted to a permanently manned station.

10.5.6 Plant specific application software

10.5.6.1 General

The design, development, verification and type approval of safety-related system with a programmable safety device (system hardware and software) is subject to Part 2 of this standard. This sub-clause covers the correct implementation of the plant-specific application software to satisfy the requirements of the safety requirements specification with respect to the required safety integrity level.

10.5.6.2 Requirements for plant-specific application software

In accordance with the required safety integrity level, the chosen programmable logic unit and its software shall satisfy the safety integrity requirements of the particular application:

– correctness of functionality;

– sequencing and time-related information;

– timing constraints;

– concurrency;

Interrupts should be avoided.

– data structures and properties;

– design assumptions and dependencies;

– testability.

The proof of the above mentioned items has to be carried out by verification and validation steps according to the design and development phases within the life cycle of the software, including

– validity of the software requirement specification,

– completeness, consistency, comprehensibility and unambiguousness of documentation and programs.

The application design representations shall be based on a notation, e.g. functional diagram, which is unambiguously defined or restricted to unambiguously defined features.

As far as practicable the application design shall minimize the safety-related part of the software.

Where the software is supposed to implement both safety and non-safety functions, then all of the software shall be treated as safety-related unless adequate independence between the functions can be demonstrated in the application design.

When implementing Application Software on a type tested platform (e.g. a PLC) the instructions of the safety manual shall be followed.

Where the software is supposed to implement safety functions of different safety integrity levels, then all of the software shall be treated as belonging to the highest safety integrity level unless adequate independence between the safety functions of the different safety integrity levels can be shown in the application design. The justification for independence shall be recorded in the relevant design documentation.

For type approved software modules the extent of testing may be limited to the tests required to ensure proper implementation. Constraints from the software environment (e.g. operating system and compiler dependencies) should be evaluated.

Depending on the nature of the software, development responsibility for conformance with this section can vary from the supplier alone, the user alone or both. The division of responsibility shall be recorded.

The proposed software architecture shall be based on a partitioning into components/sub-systems which can be identified as part of the system software and of the plant specific application software.

The following information shall be provided:

– whether they are new, existing or proprietary;

– whether they have been previously verified and if so their verification conditions;

– whether each sub-system/component is safety-related or not;

– the software safety integrity level of the sub-system/component;

– identify, evaluate and detail the significance of all hardware/software interactions;

– use a notation to represent the architecture which is unambiguously defined or restricted to unambiguously defined features;

– identify the design features used for maintaining the safety integrity of all data. This shall include: plant input-output data, communications data, operator interface data, maintenance data and internal database data.

10.5.6.3 Requirements for design

Depending on the programmable logic unit chosen, the software responsibility for conformance with this section can vary from the supplier alone, the user alone or both. The division of responsibility shall be recorded.

The safety requirements specification, the software architecture design and the requirements associated with software validation shall be available prior to the start of the detailed design process.

The software should be produced to achieve modularity, testability and maintainability.

For user application programming using a limited variability language e.g. ladder logic and function blocks, detailed design really consists of „configuring“ rather than programming. However, the software should still be designed in a structured way including

– organizing the software into a modular structure that separates out (as far as possible) safety-related parts,

– including range checking and other features that provide protection against data input errors,

– using previously verified modules,

– choosing a design that facilitates future software modifications.

For each major component/sub-system in the software architecture, further refinement of the design shall be based on a partitioning into modules.

10.5.6.4 Measures for avoiding faults

When preparing software, design and organisational precautions for the avoidance of faults shall be taken, these being, for example:

a) application of computer-aided design and development tools;

b) use of standard function modules; when doing so, the following points are to be observed:

   1) if they are to be used in the safety device, they shall be subjected to prototype testing. For software modules proven in use, the extent of prototype testing may be reduced;

   2) if they are used for operational functions, they shall have no reactions to the safety system;

c) compliance with programming guidelines when preparing system software, standard function modules and individually programmed user software; the following shall be specified:

   1) maximum nesting depth;

   2) maximum module size or complexity (dimensions);

   3) permissibility of branches and interrupts;

   4) requirements of interfaces;

   5) specifications with regard to instrumentation/plausibility checks (assertions)/monitoring of program execution.

NOTE Deviations from these programming guidelines are permissible only in justifiable individual cases.

d) application of computerised equipment for parameterisation and configuration of the user software on the basis of standard function modules;

e) development tools for application software shall be part of the safety related programmable logic controller, otherwise the development tools have to be in accordance to Part 3 of EN 61508.

10.5.6.5 Code implementation

The user application software program shall

– be readable, understandable and testable,

– satisfy its software design specification,

– satisfy the requirements of the coding manual,

– satisfy any requirements from safety planning,

– take into account the specific features of the system,

– ensure that the tested software is identical to the installed software.

NOTE For example application programming for programmable controllers may use a defined subset of the programming languages described in EN 61131–3:

– ladder diagram;

– function block diagram;

– sequential function chart;

– structured text.

10.6 Installation and commissioning

The measures of the installation and commissioning planning shall be carried out.

10.7 Safety validation

10.7.1 System integration of hardware and software

Within the programmable logic unit adequate effectiveness of the safety related system shall be ensured in accordance with Figure 12 and Figure 13. For this purpose, hardware faults and software faults (see Figure 3) shall be mastered by appropriate measures. Examples of such measures are

a) selection of a suitable system structure,

b) suitable self-tests or external tests,

c) comparing and signalling devices.

All relevant fault models shall be taken into consideration. EN 61508-2 specifies fault models and measures.

The measures for avoidance of faults which can be derived from these for hardware and software are described in 10.5.3 and 10.5.6.4.

The configuration of hardware and software shall be based on the functional analysis of the safety devices (sensor, logic unit and actuating element). The resulting design has to be structured.

In order to enhance the degree of fault detection, the following fault-management techniques should be provided, e.g.:

a) detection of faults at the outputs, e.g.:

1) comparison of input and output conditions;

2) comparison of the output conditions with the logical status of the program;

3) interlocking of output circuits within the logic unit.

b) monitoring program execution

1) with time-based program execution monitoring, this monitor shall be triggered at both the upper and the lower limit of the time interval. Faults which shift the upper and/or lower limit of the time interval shall be taken into account,

2) the application of logical program execution monitoring shall detect the omission of individual program sequences.

The reaction to identified faults shall be unambiguously specified.

10.7.2 Fault assessment for the system integration of hardware and software

Depending on the structure, requirements shall be specified for the techniques for mastering faults, consisting of techniques for fault detection and for establishing suitable reactions to these faults (see Figure 12).

Examples of system configurations are described in Annex A.

In order to achieve a required safety level with reference to EN 61508-1 depending on the duration of operation intervals (operation interval between two functional tests) and the systems structure, different degrees of fault detection are necessary.

Examples of measures to achieve the required degree of fault detection are shown in annexes.

a) within the single-channel programmable section of the safety device, hardware faults and software errors which could result in failure or malfunctions shall be detected by external or self tests

– If the effectiveness of the safety-related system is adversely affected by failure or malfunctions, triggering of the safety device shall be induced,

– In such a case the total of the time for fault detection and the time for triggering the device shall always be less than the fault tolerance time (see Figure 14). The time for fault detection results from the sum of the test cycle time and the testing time for self tests or external tests.

b) For those parts of the safety related system which are in a multi-channel configuration, the effectiveness of the safety related system shall be retained in full even following the occurrence of a fault

– in order to protect against multiple faults, all those hardware faults or software errors which could lead to outages or malfunctions shall be detected, or the effectiveness of the safety related system shall be maintained even in the event of a fault in the second channel. In order to have a high success rate for the fault detection procedure, a results comparison of the channels (protection against active faults) and external and/or self tests (protection against passive faults) shall be conducted. The components for the results comparison as well as the external or self test (hardware and software) shall likewise be provided with fault detection means, and a fault signal shall be generated to permit its correction,

– the maximum permissible time for the detection and correction of faults depends on the required safety integrity level and the probability that a fault will occur in a further channel, which together with the defective first channel will compromise the effectiveness of the safety related system. If within this time the fault is not corrected, shutdown of the plant in a safe way shall be initiated.

Should the effectiveness of the safety related system be retained in the event of a fault in the second channel, and if the faults in both channels are not automatically detected, the faults shall be detected in sufficient time by periodic testing, and then cleared.

NOTE The maximum permissible time for fault detection and clearance is as a rule several orders of magnitude greater than the corresponding fault tolerance time and may be from hours to days.

The time-interval between periodic tests (inspection interval) shall be determined by the protection equipment design, it shall also take into account the manufacturer's specification for individual safety devices.

10.7.3 Type approval

Subsystems, such as modules for modular systems are likewise considered safe if type approval as stipulated in Part 2 of this standard or relevant safety standard has been conducted by a testing laboratory accredited for these devices. For the use of type approved subsystems as part of the safety-related system, the entire application shall be assessed in accordance with Figure 11, Figure 12 and Figure 13. Additional assessment for the type approved subsystem is not necessary. The safety manuals of the subsystems have to be considered.

10.7.4 Plant-specific test

Plant-specific tests according to Part 3 of this standard shall validate that the safety-related system meets all specified requirements. These shall include the correct implementation of the logic unit (hardware and software modules), field devices and their interconnections. The safety manuals of the subsystems or devices have to be considered.

All safety functions shall undergo function tests at least once during implementation (commissioning). Safety functions shall be tested periodically to ensure that these functions are not impaired by undetected faults.

The maximum period between two function tests depends on

– the required safety integrity level,

– the configuration of sensors and actuating elements (see Table 1),

– the configuration of the logic system, e.g. programmable safety device (see Annex A),

– the diagnostic coverage.

The function tests shall include sensors, logic unit and actuating elements. The function test shall be carried out as a complete test at a time or by overlapping partial tests (e.g. sequential single channel test of a multi-channel arrangement, sequential tests of sensors, logic solver and actuating elements). The overlapping shall ensure that the partial tests cover the complete function.

Examples of the interval of operation between two function tests are given in Table 1 for common combinations of field devices (sensors and/or actuating elements) and in Annex A for configurations of logic units.

NOTE Some European countries have legal requirements for third party tests for specific applications (e.g. steam boilers).

10.8 Operation and maintenance

The supplier shall define the requirements to ensure the safety of the safety-related system is maintained during operation and maintenance. This shall include the requirements to function test the protection system at defined intervals.

Operation and maintenance requirements shall be defined and documented which shall include the following:

- the routine actions which are needed to function test the protection system;

- any actions and constraints that are necessary (e.g. during start-up, normal operation, routine testing, foreseeable disturbances, faults or failures, and shutdown) to prevent an unsafe state and/or reduce the consequences of the hazard;

- information on procedures to be followed when faults or failures occur, including procedures for fault diagnoses and repair;

- identify tools necessary for maintenance and requirements for maintaining the tools and equipment

- the requirements laid down in the manuals (to be provided by the device vendors) of the different devices (e.g. special activities like inspections of breakers after occurrence of a short).

10.9 Modification and retrofit

10.9.1 General

Modifications to the protection system shall not be carried out unless the modification is verified concerning

- the reasons for the change shall be identified,

- the hazards shall be identified which may be affected,

- the proposed change of both hardware and software shall be detailed,

- an assessment of the impact on safety shall be carried out.

Depending on the nature and extent of the change, and its impact on safety, the modification may require authorization, a return to the appropriate phase of the lifecycle and retesting. The extent to which a system is retested will vary depending on the modification, however, many changes will require a complete retest of the safety related system in accordance with Part 3 of this standard.

10.9.2 Measures against unauthorised changes or overriding

In the case of the safety-related systems, appropriate precautions shall be taken to prevent unintentional or unauthorised modifications or overriding of safety functions, for example, during simulation exercises.

NOTE Constructional precautions for this purpose are preferred, for example:

– installation in housings which can only be opened with a tool;

– installation in locked cabinets or rooms;

– access to programming facilities restricted to those with appropriate tool, key or password.

Where constructional precautions cannot be implemented, organisational precautions should be used, for example:

– authorization rules, key rules;

– written job orders, entry into logbooks;

– monitoring of cabinet doors.

11 Electrical equipment

11.1 General requirements

Electrical equipment including other equipment with electrical assemblies shall satisfy the applicable standards; it shall be suitable for its intended purpose.

Electrical equipment shall be installed and mounted so that normal operation and maintenance is possible without danger to operators.

The mounting location, direction of actuation and connection of electrical equipment shall conform to the manufacturer's data.

Electrical equipment which is to be operated at variable frequencies shall be designed so that its functional performance is unaffected by phenomena such as overvoltages, voltages and current waveforms, which is dependent upon the loading of the circuit.

11.2 Creepage distances and clearances

Electrical equipment shall at least meet the requirements of Pollution Degree 3 and Overvoltage Category III as specified in EN 60664-1.

Alternatively electrical equipment may be designed for Pollution Degree 2 if it is fitted in enclosures which conform to at least class of protection IP54 in accordance with EN 60529 or if it is installed in dry and clean rooms.

Terminals and plug-and-socket connections for the connection of cables and cords at the place of use shall be equivalent to Pollution Degree 3 and Overvoltage Category III in accordance with EN 60664-1.

For equipment with electronic equipment, the creepage distances and clearances in EN 60664-1 should be used. This also applies to printed circuits boards with other equipment.

11.3 Motors

Electric motors shall conform to standards in the EN 60034 series.

Motors shall at least meet the requirements of class of protection IP44 in accordance with EN 60529, except where specified below.

When selecting the operating mode, the most unfavourable mode of operation shall be taken as a basis.

Motors for burners shall be designed together with the burner blower for continuous operation (operating mode S1). They shall at least meet the requirements of class of protection IP21 in accordance with EN 60529 with a maximum slot width of 8 mm.

11.4 Transformers

For control and ignition transformers, where no IEC standard exists, national standards shall remain valid, until CENELEC requirements become available, provided that the relevant national standards refer specifically to the equipment dealt with in this EN.

Ignition transformers including accessories on the high-voltage side shall at least meet the requirements of class of protection IP4X in accordance with EN 60529. When used in the open air, they shall at least meet the requirements of class of protection IP54 in accordance with EN 60529.

Ignition transformers shall be designed for a 100 % duty ratio in the case of continuous ignition operation.

Ignition devices with high-voltage capacitors in the high-voltage section shall be equipped with a permanently installed discharge device with the discharge time being not longer than 2 min.

NOTE In the case of discharge times of more than 1 mi, information plate HS1 as specified in EC Directive 92/58/EWG may be necessary.

Isolating transformers for the control supply for safety extra-low voltage (SELV) circuits shall conform to EN 61558-1 equipment which is defined in HD 60364.

11.5 Switching devices

Contactors shall conform to EN 60947-4-1 and relays shall conform to EN 61810-1.

Other relays may only be mounted in electrical equipment for furnaces if they are used within an electrical module or a structurally enclosed unit (e.g. several modules in sub-rack).

The contacts of electromechanical equipment shall achieve a mechanical endurance of at least 250 000 switching cycles in accordance with EN 60947-4-1.

Circuit breakers shall conform to EN 60947-2.

11.6 Operator control devices

The requirements in 4.2.1 shall be observed with regard to the design and function of operator control devices.

Contact elements of automatic control systems and limiters shall be of the snap-action type.

11.7 Immersion electrodes

When using immersion electrodes, the following conditions shall be fulfilled:

Control circuits with immersion electrodes shall be electrically isolated from other auxiliary circuits and from the mains supply. They shall not be operated with an earth, apart from the obligatory earthing in the return line via the cover flange.

The operating voltage of electrodes shall not exceed 50 V. The voltage shall be supplied by an isolating transformer in accordance with EN 61558-1 which shall satisfy the requirements of class of protection II (total insulation) and class of protection IP55 in accordance with EN 60529.

In the case of a completely immersed electrode head, the current density at the electrode shall not exceed 10 mA per cm^2 of electrode surface.

Immersion electrodes may be used with two electrodes connected in series or with one electrode with the metal structure of the boiler being used as the counter electrode. If only one electrode is used, the return line shall be directly connected to the cover flange of the immersion electrode.

11.8 Trace heating systems

Standards in the EN 60519 series shall be observed in respect of the electric heating of intermediate vessels and pipelines.

12 Cables and cords

12.1 General requirements

Only cables and cords which are made of materials which are at least flame-inhibiting or self-extinguishing according to EN 60332-1-1 and EN 60332-2-1 shall be used.

Conductors, cables and cords shall be selected so that they are suitable for the prevailing operating conditions (e.g. voltage, current, protection against electrical shock) and environmental conditions (e.g. ambient temperature).

When installed, cables and cords should have sufficient strength against mechanical damage. Where the risk of damage can be foreseen, cables shall preferably be routed elsewhere, or provided with additional protection.

The ends of stranded, finely stranded and extra finely stranded conductors shall be secured e.g. by means of wire end ferrules, cable lugs or appropriate design of the terminals, to prevent stray strands making contact with other conductors.

The minimum cross-sectional area for control and signalling conductors shall be matched to suit the selected method for terminal connections.

Only cables and cords should be used which conform to the relevant EN or IEC standards or which are equivalent to those.

On ships only cords and cables which conform to the particular standards for ships may be used.

12.2 Insulation

The disruptive strength of the insulation shall be designed for the required test voltage. In circuits with voltages exceeding AC 50 V, only cables and cords shall be used which are tested in accordance with the relevant EN and IEC Specifications with a voltage of at least AC 2 000 V.

In the case of voltages up to AC 50 V, the test voltage shall be at least AC 500 V wire/wire and AC 2 000 V wire/screen.

The mechanical strength and the thickness of the insulation shall be such that the insulation may not be damaged during operation or installation, especially for cables to be laid into ducts or drawn into conduits.

12.3 Current-carrying capacity

Requirements in the relevant EN and IEC standards are applicable to the current carrying capacity as a function of conductor cross-sectional area.

The cross-sectional areas for copper conductors shall not be less than the following values:

a) Cords outside enclosures, outside electrical operating areas and closed electrical operating areas:

   1) 0,75 mm^2 for cords with 2 stranded cores;

   2) 0,5 mm^2 for cords with 3 or more cores and for screened twin or multi-core cords;

b) Cords inside enclosures: 0,2 mm^2;

c) Inside enclosures, conductors with cross-sectional areas less than 0,2 mm^2 may be used to connect electronic components provided that correct functioning is ensured.

On ships, the relevant EN or IEC standards are applicable for the current-carrying capacity of the external wiring.

Condition c) is not applicable on ships.

The maximum permissible operating temperature on the conductor of cables and cords (ambient temperature plus overtemperature) shall not exceed the permissible limit temperature of the insulation in accordance with EN or IEC specifications.

12.4 Conductors of separate circuits

Conductors of different circuits may be laid side by side, may occupy the same duct (e.g. conduit cable trunking system) or may be in the same multi-conductor cable, providing that the arrangement does not

impair the proper functioning of the respective circuits. Where these circuits operate at different voltages, the conductors shall be either separated by suitable barriers or insulated for the highest voltage to which any conductor in the same duct can be subjected.

13 Warning signs and item designation

13.1 Warning signs

Enclosures which do not clearly show that they contain electrical devices shall be marked with a black lightning flash on a yellow background within a black triangle, shaped in accordance with IEC 60417-DB-symbol 5036 (applied as warning sign according to ISO 3864 series).

This warning sign shall be durably fixed to electrical control enclosures which

– do not have the supply disconnecting device integral with the enclosure,

– contain more than one electrical device,

– are not connection or junction boxes.

Warning signs shall be

– attached to the enclosure door or cover,

– plainly visible to all operating personnel.

13.2 Functional identification

Control devices, visual indicators, terminals and displays (particularly those related to safety functions) shall be clearly and durably marked with regard to their functions either on or adjacent to the unit.

This does not apply to symbols in (mosaic) mimic diagrams and displays on video control consoles.

Depending on the complexity of the installation, tagging of components should also apply for cables, hock ups, terminal boxes, etc.

13.3 Item designations

All control devices and components shall be plainly identified with the same designation as shown in the technical documentation. This identification shall be in accordance with EN 81346-1.

Where size or location preclude the use of individual item designation, group designation shall be used.

14 Technical documentation

14.1 General

In the documentation, those parts which are relevant to safety functions shall be clearly identified. The documentation has to be

– easy to follow,

– logically structured,

– readily comprehensible.

14.2 Documentation describing functions and connections

14.2.1 General

Documentation relating to the electrical equipment clearly showing its method of operation and construction is required. Equipment, connections, wiring and signals shall be consistently identified in all associated documents. The circuit documentation and graphical symbols shall conform to the relevant EN and IEC standards, e.g. IEC 60617 and EN 61082-1.

14.2.2 Documentation describing functions

Circuit documentation to explain the mode of operation, such as

– overview diagrams,

– function diagrams,

– block diagrams,

– descriptions of equipment,

– P + I schematics (piping or process equipment and instrumentation schematics),

– schematic diagrams,

– flow charts,

– time sequence charts,

– operating instructions,

– maintenance and fault finding instructions.

14.2.3 Documentation describing connections

Circuit documentation to explain connections and physical layout such as

– internal wiring diagrams,

– external connection diagrams,

– terminal connection diagrams,

– location diagrams,

– lists of measuring points and loads,

– instrument loop diagrams.

14.2.4 Documentation describing the process

Description of process including sufficient detail to enable a competent person to identify the cause of any furnace shutdown.

14.2.5 Documentation of the risk assessment

The risk assessment and the resulting required safety integrity level shall be documented, describing all the considered facts.

14.3 Documents for type approved components

For type approved assemblies, such as burner control systems, safety limiters and flame monitoring devices, it suffices to

– provide a terminal wiring diagram,

– supply instructions for installation, operation and, where appropriate, maintenance.

For type approved modular systems, such as programmable safety device additional documents are necessary, e.g.:

– approval (certificate and test expertise);

– listing of pretested devices and modules;

– safety manual according EN 61508-4;

– user manual.

14.4 Documentation of the application software

In the documentation of the application software, all implemented functions (at application level) performed in the program shall be described completely and with no inconsistencies.

Preferably, application-oriented graphical presentation should be used (e.g. functional diagrams)

An essential part of the documentation of the applications software is a clear designation of the issue (state of revision). The documentation shall comprise the following details:

– general operational parameters (e.g. cycle time, process safety time, time until occurrence of additional second fault);

– presentation of system hardware (modules);

– documentation of user-configurable hardware test procedures;

– documentation of allocations of signals to hardware channels;

– cross reference list, if applicable;

– documentation of implemented functions at application level;

– documentation of internal software variables (markers, flags).

Annex A
(informative)
Configurations of programmable safety devices (PSD) with reference to EN 61508

A.1 General

The following configurations are examples of applications of PSD which are used to realize safety functions. Those systems are not taken into account which increase the availability using additional redundant structures (e.g. structure 1oo1 in parallel) based on the following configurations.

The description is confined to the signal processing units, to the monitoring equipment and to the output configurations. For the input configurations, it is supposed that the connections of the input channels are according to that of the output channels (all safety-relevant inputs are connected in parallel to all signal processing units, e.g. 2oo3 configurations).

Explanation of symbols used in the following pictures:

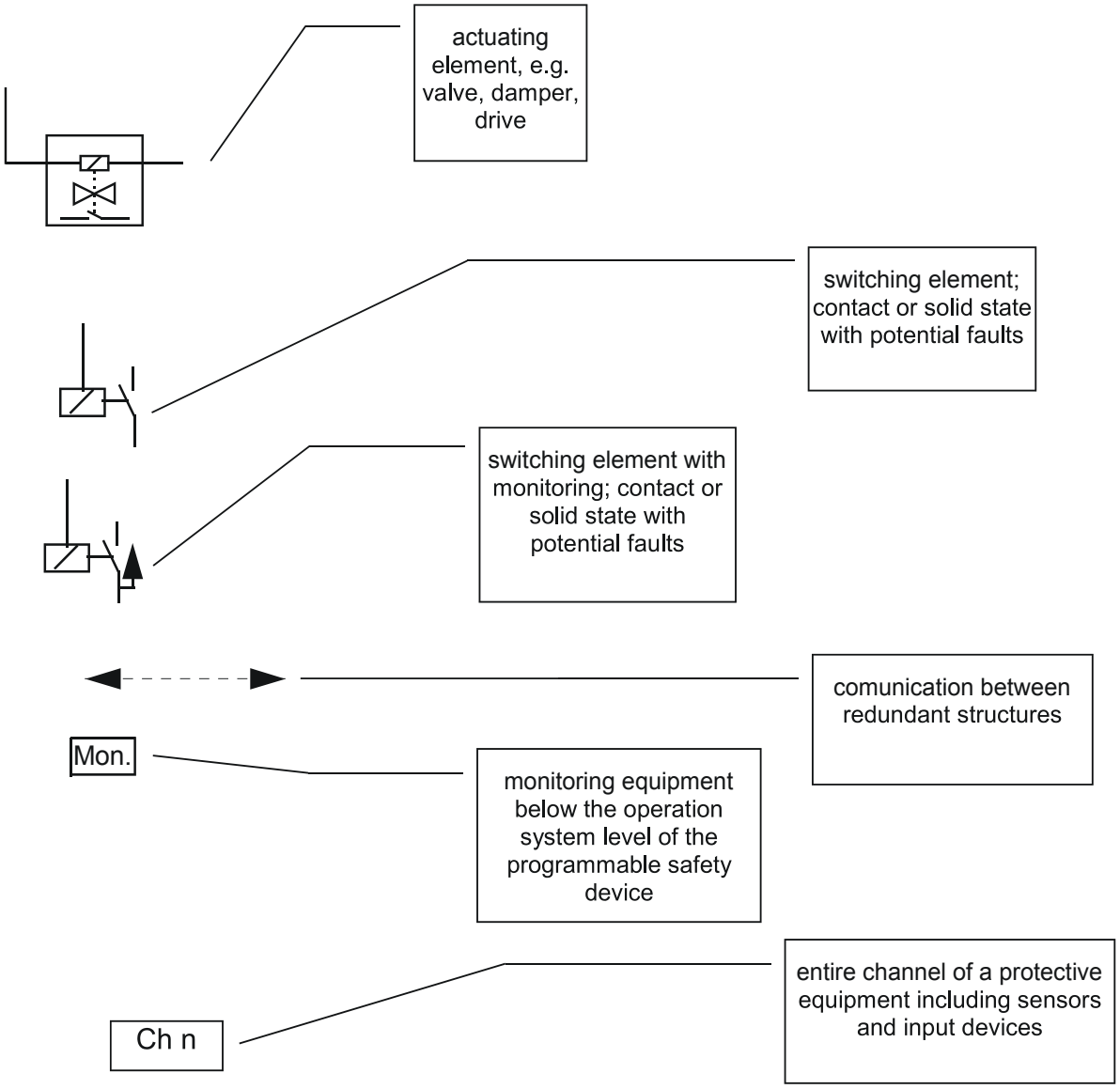


Figure A.1 - Explanation of symbols

A.2 Configuration 1oo1

Features:

Configuration consisting of single channel CPU and monitoring. Two switching elements with monitoring for the safety function.

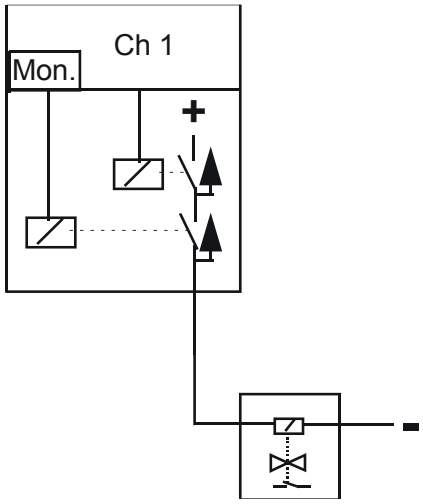


Figure A.2

Modes of operation

Table A.1

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage
1	≤ 1 month	None
1	≤ 6 months	Simple
1	≤ 1 year [a]	Medium
2	≤ 1 month	Medium
2	≤ 6 months	high-grade

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

Assumptions:

Detection of dangerous primary faults within process safety time.

Detection of multiple faults within the time of second faults occurrence.

A.3 Configuration 1oo1D

Features:

Configuration consisting of double channel CPU, comparison and monitoring. Two switching elements with monitoring for the safety function.

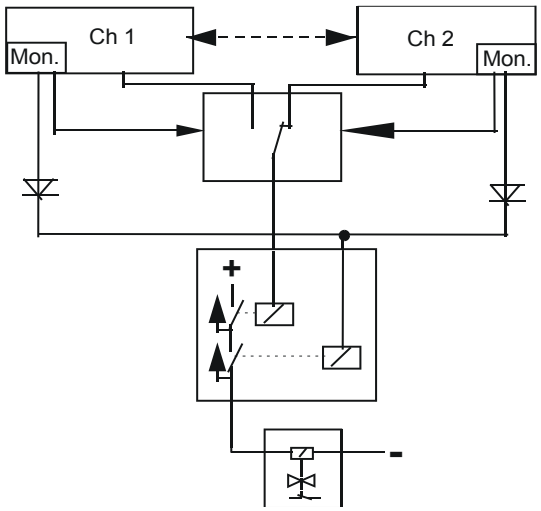


Figure A.3

Modes of operation

Table A.2

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage
1	≤ 1 month	simple
1	≤ 6 months	medium
1	≤ 1 year [a]	high-grade
2	≤ 1 month	medium
2	≤ 6 months	high-grade

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

Assumptions:

Detection of dangerous primary faults within process safety time,

Detection of multiple faults within the time of second faults occurrence.

Possibly increasing of the diagnostic coverage of the signal processing units using comparison of data and diagnostic results.

A.4 Configuration 1oo2

Features:

Double-channel system. The output circuits are configured in such a way that one of both systems can trigger a shut-down of the entire system.

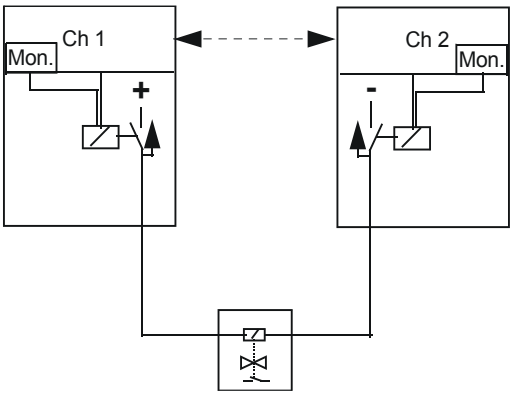


Figure A.4

Modes of operation

Table A.3

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage
2	≤ = 6 months	none
2	≤ 1 year [a]	medium
3	≤ 1 month	none [c]
3	≤ 6 months	simple [c]
3	≤ 1 year [b]	medium [c]

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

[c] Permissible if numerical fault analysis has been carried out to prove reliability; otherwise high diagnostic coverage is necessary.

Assumptions:

Detection of dangerous primary faults within the time of second faults occurrence,

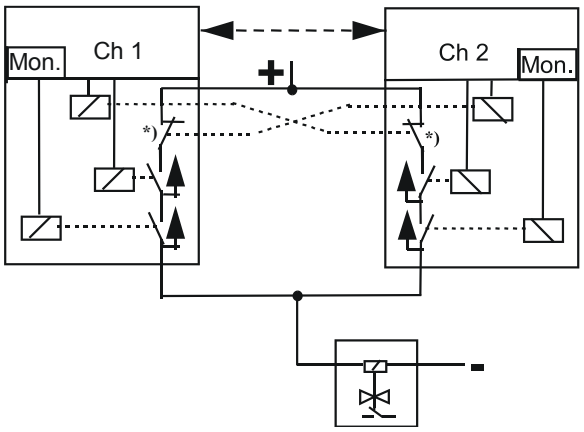
Detection of multiple faults within the time of second faults occurrence.

Possibly increasing of the diagnostic coverage of the signal processing units using comparison of data and diagnostic results.

A.5 Configuration 1oo2D

Features:

Double-channel configuration with double channel I/O and double channel signal processing units, including communication between the signal processing units.



Key

*) additional tripping possibility by crosswise switching of the redundant partial system

Figure A.5

Modes of operation

Table A.4

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage
2	≤ 6 months	None
2	≤ 1 year [a]	Medium
3	≤ 1 month	none [c]
3	≤ 6 months	simple [c]
3	≤ 1 year [b]	medium [c]

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

[c] Permissible if numerical fault analysis has been carried out to prove reliability; otherwise high diagnostic coverage is necessary.

Assumptions:

Detection of dangerous primary faults within the process safety time.

Detection of multiple faults within the time of second faults occurrence.

Possibly increasing of the diagnostic coverage of the signal processing units using comparison of data and diagnostic results.

A.6 Configuration 2oo3

Features:

2oo3 system with mutual monitoring of data and self-monitoring of the channels.

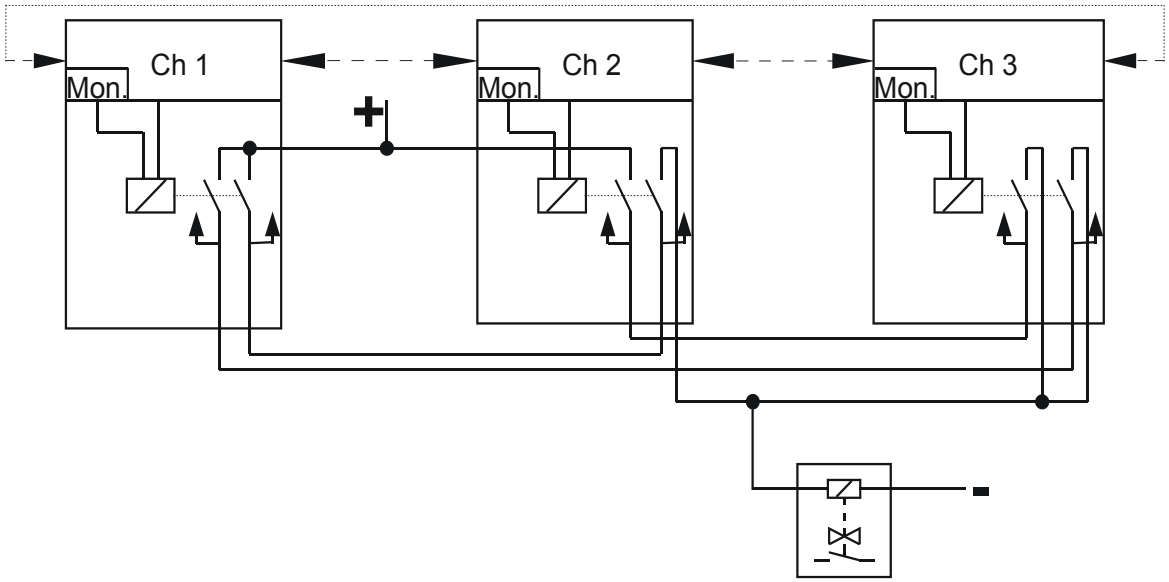


Figure A.6

Modes of operation

Table A.5

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage [a]
2	≤ 1 month	None
2	≤ 1 year [a]	Simple
3	≤ 1 month	none [c]
3	≤ 6 months	simple [c]
3	≤ 1 year [a]	medium [c]

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

[c] Permissible if numerical fault analysis has been carried out to prove reliability; otherwise high diagnostic coverage is necessary.

Assumptions:

Detection of dangerous primary faults within the time of second faults occurrence.

Detection of multiple faults within the time of second faults occurrence.

Allowance of a two channel operation for a limited time.

A.7 Configuration 2oo3D

Features:

2oo3 system with mutual monitoring of data and self-monitoring of the channels.

Two independent tripping paths for each channel.

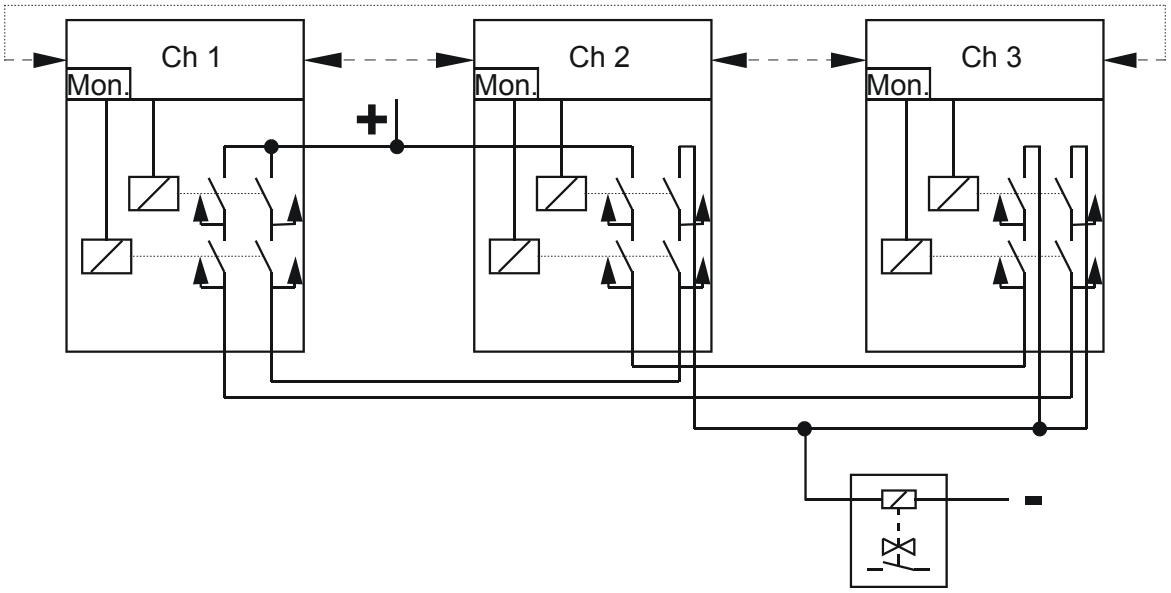


Figure A.7

Modes of operation

Table A.6

Safety integrity level	Interval of operation between two functional tests [b]	Diagnostic coverage
2	≤ 1 month	None
2	≤ 1 year [a]	Simple
3	≤ 1 month	none [c]
3	≤ 6 months	simple [c]
3	≤ 1 year [a]	medium [c]

[a] Longer intervals are possible concerning the safety-related system.

[b] Functional test to prove the function of the safety related system.

[c] Permissible if numerical fault analysis has been carried out to prove reliability; otherwise high diagnostic coverage is necessary.

Assumptions:

Detection of dangerous primary faults within the time of second faults occurrence.

Detection of multiple faults within the time of second faults occurrence.

Allowance of a two channel operation for an unlimited time.

Annex B
(informative)
Lifecycle of programmable safety device

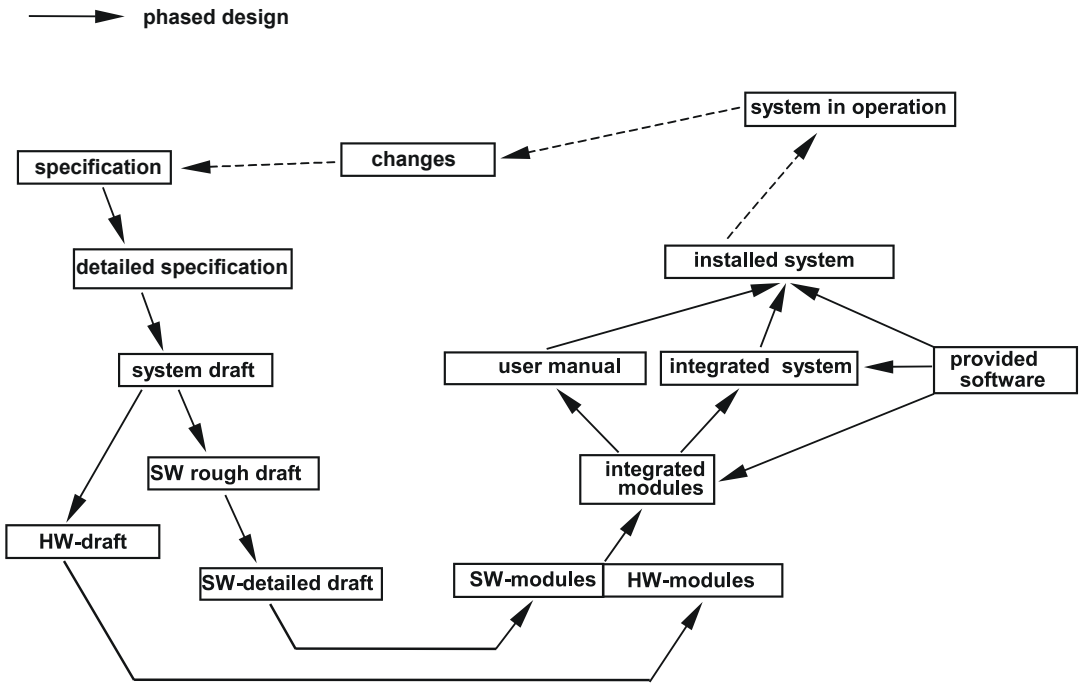


Figure B.1

Annex C
(informative)
Management of functional safety

Management of functional safety shall be carried out throughout the safety lifecycle for the application, design and installation of a furnace safety-related system (see Figure 8).

Management of functional safety shall specify all the management and technical activities during the safety lifecycle phases which are necessary to ensure that the safety-related systems achieve and maintain the required functional safety. Also, the responsibilities of the persons, departments and organizations for each lifecycle phase or for activities within each phase should be specified.

In particular, following items should be considered:

– The policy and strategy for achieving safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;

– Identification of the persons, departments, organisations or other units which are responsible for carrying out and reviewing each of the design and installation process phases (including, where relevant, licensing authorities or safety regulatory bodies);

– The selected measures and techniques used to meet the requirements of a specified clause in this standard (see 10.5.2 and 10.5.3);

– The procedures for ensuring prompt follow-up and satisfactory resolution of recommendations arising from

  – hazard and risk analysis,

  – verification, validation and testing activities,

  – configuration management and change control procedures;

– The procedures for ensuring all staff involved in all design and installation process activities are competent to carry out activities for which they are accountable;

– The plans for identifying and dealing with cases of faults or failures which result in diminished capacity to perform activities necessary for achieving functional safety;

– The procedures for monitoring systematic fault experience (both hardware and software) of existing installations and modifications as a result of identifying faults which could compromise the safety of furnace installations;

– The procedures for identification of all relevant items (both hardware and software) and their documentation. Each item shall have a unique identification and each version of the item shall be identified.

This is an non-exhaustive list of the requirements for the management of functional safety and further information on this topic is provided in EN 61508-1:2010, Clause 6.

Annex D
(informative)
Examples of determining the safety integrity level SIL using the risk graph method

D.1 General

A hazard and risk analysis shall be carried out for each hazard to the furnace and the heated system. Requirements in terms of the composition of the team are described in Section 10.3.

The team normally considers consecutively each safety-related function of the furnace and the heated system. When selecting the parameters which lead to a lower risk (e.g. F1 instead of F2), all the relevant arguments and grounds shall be listed. Arguments shall not lead to the reduction of several parameters. The results of the SIL determination with the decisions made and grounds shall be documented in writing. These documents shall be confirmed by the parties involved and shall be subject to version management.

NOTE Environmental hazards or damage to property are not taken into account in the risk graph (Figure 9). In this regard, reference is made to DIN VDE 61511–3, Section D.7 or D.8.

D.2 Risk parameter C (Consequences of the hazardous event)

When describing the hazard, the cause of the hazardous situation shall also always be stated. For example, the explosion of the boiler pressure body may be brought about by a wide variety of causes such as overheating with a lack of water, excess pressure as a result of continuous heating, explosion in the furnace as a result of a dangerous fuel/air ratio, etc. Each of these causes is then assigned at least one safety-related function which then shall reduce the resultant risk. The worst case scenario shall be taken into account.

D.3 Risk parameter F (Frequence and duration of the time spent in the hazard area)

The factor of time spent shall be determined on the basis of the person most exposed to the risk, not the average of all persons. It is thus ensured that the risk is not averaged out across all persons.

D.4 Risk parameter P (Possibility of preventing the hazardous event)

P1 should only be used if all the following statements correspondingly apply:

– the risk is apparent before it fully enfolds;

– the time that passes after detection until full occurrence of the hazard is definitely sufficient to carry out the necessary tasks;

– independent devices are present by means of which the risk can be avoided by the operator or it is possible for all persons to flee from the hazard area.

D.5 Risk parameter W (Likelihood of occurrence of the hazardous event)

Risk parameter W encompasses the likelihood of occurrence of the hazardous procedural state in the absence of the safety-related function to be classified. Measures which are entirely independent of the safety function to avoid this specific risk can be taken into account in reducing W. When quantifying W, the following requirement rates can be assumed:

– W1 very low (lower than 1x in 10 years);

– W2 low (1x in 10 years to 1x in a year);

– W3 relatively high (1x to 10x in a year).

When applying the standard, the mode of operation with a lower requirement rate generally applies. If W3 is determined, the mode of operation with a continuous requirement is already present.

Bibliography

EN 50160:2010, *Voltage characteristics of electricity supplied by public electricity networks*

EN 60519-1:2011, *Safety in electroheating installations - Part 1: General requirements (IEC 60519-1:2010)*

EN 61131-3:2003, *Programmable controllers - Part 3: Programming languages (IEC 61131-3:2003)*

EN 61140: 2002, *Protection against electric shock - Common aspects for installation and equipment (IEC 61140:2001)*

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

EN 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations (IEC 61508-4:2010)*

EN 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5:2010)*

EN 60204-1:2006, *Safety of machinery - Electrical equipment of machines - Part 1: General requirements (IEC 60204-1:2005, mod.)*

HD 60364-5-54:2011, *Low-voltage electrical installations – Part 5-54: Selection and erection of electrical equipment – Earthing arrangements, protective conductors and protective bonding conductors (IEC 60364-5-54:2011)*

EN ISO 13850:2008, *Safety of machinery - Emergency stop - Principles for design (ISO 13850:2006)*

IEC 60092-101:1994, *Electrical installations in ships – Part 101: Definitions and general requirements*

IEC 60050-191:1990, *International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service, ed. 1.0*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™