INTERNATIONAL STANDARD

ISO 13577-4

Second edition
2022-07

Industrial furnaces and associated processing equipment — Safety —

Part 4: Protective systems

Fours industriels et équipements associés — Sécurité —

Partie 4: Systèmes de protection

Reference number
ISO 13577-4:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 244, *Industrial furnaces and associated processing equipment*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 186, *Industrial thermoprocessing - Safety*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO 13577-4:2014), which has been technically revised.

The main changes are as follows:

— to provided better clarity methods B and C were combined to create a new method BC,

— Annex E was rewritten to provide several new examples to better reflect the intent for previously misunderstood elements,

— Annex B was modified to include clearer language and examples of normative wiring. The original Annex F was merged,

— created wording to provide a better alignment with IEC 62061, IEC 61511, and ISO 13849-1.

A list of all parts in the ISO 13577 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document was developed to specify the requirements of a protective system, which is a safety-related control system (SCS) of industrial furnaces and associated processing equipment (TPE). It is intended that in designing the protective system of TPE, manufacturers of TPE choose from the three methods provided in this document. Requirements for safety-related control functions of TPE are specified in ISO 13577-1, ISO 13577-2, and ISO 13577-3.

This document is intended to be used jointly with ISO 13577-1, ISO 13577-2 and ISO 13577-3. Since the other parts of the ISO 13577 series are type-C standards of ISO 12100, TPE are required to be designed in accordance with the principles of ISO 12100. The type-B standards of ISO 12100 for SCS are IEC 62061 or ISO 13849-1, which always assume high-demand applications. However, there are cases in which a risk assessment according to the IEC 61511 series, which provides the option of a low-demand rate on the protective system, is more suitable for the design of a TPE protective system.

In principle, when requirements of ISO 13577-1, ISO 13577-2 and ISO 13577-3 (type-C standards) are different from those which are stated in type-A or -B standards, the requirements of the type-C standards take precedence over the requirements of the other standards for machines, which have been designed and built according to the requirements of the type-C standards. Therefore, this document permits risk assessment for safety-related electrical control systems (SRECS) in which risk assessment based on the IEC 61511 series can be chosen as an alternative.

Industrial furnaces and associated processing equipment — Safety —

Part 4: Protective systems

1 Scope

This document specifies the requirements for protective systems used in industrial furnaces and associated processing equipment (TPE).

The functional requirements to which the protective systems apply are specified in ISO 13577-1 ISO 13577-2 and ISO 13577-3.

This document is not applicable to blast furnaces, converters (in steel plants), boilers, fired heaters (including reformer furnaces) in the petrochemical and chemical industries.

This document is not applicable to electrical cabling and power cabling upstream of the TPE control panel/protective system.

This document is not applicable to the protective systems manufactured before the date of its publication.

2 Normative references

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

ISO 13574, *Industrial furnaces and associated processing equipment — Vocabulary*

ISO 13849-1:—,[1)] *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

IEC 60947-4-1:2018, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters*

IEC 60947-5-1:2016, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices*

IEC 60204-1:2016, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

IEC 60730-2-5:2013+AMD1:2017+AMD2:2020 CSV, *Automatic electrical controls for household and similar use — Part 2-5: Particular requirements for automatic electrical burner control systems*

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

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

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

1) Fourth edition under preparation. Stage at the time of publication: ISO/DIS 13849-1:2022.

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

IEC 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 61508-6:2010, *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 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

IEC 61131-3:2013, *Programmable controllers — Part 3: Programming languages*

IEC 61511-1:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements*

IEC 61511-2:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1:2016*

IEC 61511-3:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels*

IEC 62061:2021, *Safety of machinery - Functional safety of safety-related control systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13574 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
final element
part of a *protective system* (3.6), that implements the physical action necessary to achieve or maintain a safe state

Note 1 to entry: Examples are valves, switch gears, and motors, including their auxiliary elements, for example, a solenoid valve and actuator if involved in the safety function.

[SOURCE: IEC 61511-1:2016, 3.2.22, modified — "BPCS or SIS" has been changed to read "protective system" in the definition.]

3.2
flame detector device
device by which the presence of a flame is detected and signalled

Note 1 to entry: It can consist of a flame *sensor* (3.9), an amplifier, and a relay for signal transmission.

[SOURCE: ISO 13574:2015, 2.65, modified — The second sentence in the original definition is presented as Note 1 to entry.]

3.3
logic function
function which performs the transformations between input information [provided by one or more input functions or *sensors* (3.9)] and output information [used by one or more output functions or *final elements* (3.1)]

Note 1 to entry: Logic functions are executed by the *logic solver* (3.4) of a *protective system* (3.6).

[SOURCE: IEC 61511-1:2016, 3.2.35, modified — "input functions" has been changed to read "input functions or sensors" and "output function" had been changed to read "output function or final elements" in the definition; Notes 1 and 2 to entry in the original definition had been deleted and Note 1 to entry has been added.]

3.4
logic solver
part of a *protective system* (3.6) that performs one or more *logic function(s)* (3.3)

Note 1 to entry: Examples are electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. *Sensors* (3.9) and *final elements* (3.1) are not part of the logic solver.

[SOURCE: IEC 61511-1:2016, 3.2.36, modified — "either a BPCS or SIS" has been changed to read "a protective system" in the definition; Note 1 to entry in the original definition has been deleted.]

3.5
programmable (logic) controller
PLC
digitally operating electronic operating system, designed for use in an industrial environment, which uses a programmable memory for the internal storage of user-oriented instructions to implement specific functions such as logic, sequencing, timing, counting and arithmetic, to control, through digital and analogue inputs and outputs, various types of machines or processes

[SOURCE: IEC 61131-1:2003, 3.5, modified — The second sentence of the original definition and Note 1 to entry have been deleted.]

3.6
protective system
instrumented system used to implement one or more safety-related instrumented functions which is composed of any combination of *sensor(s)* (3.9), *logic solver(s)* (3.4), and *final elements* (3.1)

Note 1 to entry: This can include safety-related instrumented control functions or safety-related instrumented protection functions or both.

Note 2 to entry: For example, see Figure 2.

[SOURCE: ISO 13574:2015, 2.138, modified — Note 1 to entry has been merged with the definition.]

3.7
safety bus
bus system and/or protocol for digital network communication between *safety devices* (3.8), which is designed to achieve and/or maintain a safe state of the *protective system* (3.6)

[SOURCE: ISO 13574:2015, 2.164]

3.8
safety device
device that is used to perform protective functions, either on its own or as a part of a *protective system* (3.6)

EXAMPLE *Sensors* (3.9), limiters, flame monitors, burner control systems, logic systems, *final elements* (3.1), and automatic shut-off valves.

3.9
sensor
device that produces a signal based on a process variable

EXAMPLE Transmitters, transducers, process switches, and position switches.

3.10
system for permanent operation
system, which is intended to remain in the running position for longer than 24 h without interruption

[SOURCE: IEC 60730-2-5:2013+AMD1:2017+AMD2:2020 CSV, 2.5.101]

3.11
system for non-permanent operation
system, which is intended to remain in the running position for less than 24 h

[SOURCE: IEC 60730-2-5:2013+AMD1:2017+AMD2:2020 CSV, 2.5.102]

4 Design requirements for equipment in a protective system

4.1 General

Electrical installations and equipment shall comply with IEC 60204-1:2016 and withstand the intended operating stresses and external influences and hazards identified in the risk assessment required at the design stage. Electrical installation and equipment shall be protected against damage. In particular, it shall be robust to withstand damage during continuous operation.

Devices shall be used in accordance with their instructions including safety manuals. Any device used outside of its published instructions shall be verified and validated to be suitable for the intended application.

Devices of a protective system shall withstand the environmental conditions according to IEC 60204-1:2016, 4.4 and fulfil their intended function.

Sensors (e.g. pressure transmitters, temperature transmitters, flow transmitters) used in the protective system shall be independent from the process control system.

NOTE 1 Operating information can be exchanged but cannot compromise the functional safety of the protective system.

Safe state shall be realized by de-energized circuits only.

Functional safety requirement, as identified in the ISO 13577 series shall be in accordance with the IEC 61508:2010 series, the IEC 61511:2016 series, IEC 62061:2021 or ISO 13849-1:—[2] as applicable, and implemented with the required SIL/PL for each function.

For the determination of the performance level of a safety function according to ISO 13849-1:—, the alternative procedure as stated in ISO 13849-1:—, 6.1.9 is not allowed.

Figure 1 is provided as an aid to understand the relationship between the various elements of TPE and their ancillary equipment, the heating system, the process control system and the protective system.

2) Fourth edition under preparation. Stage at the time of publication: ISO/DIS 13849-1:2022.

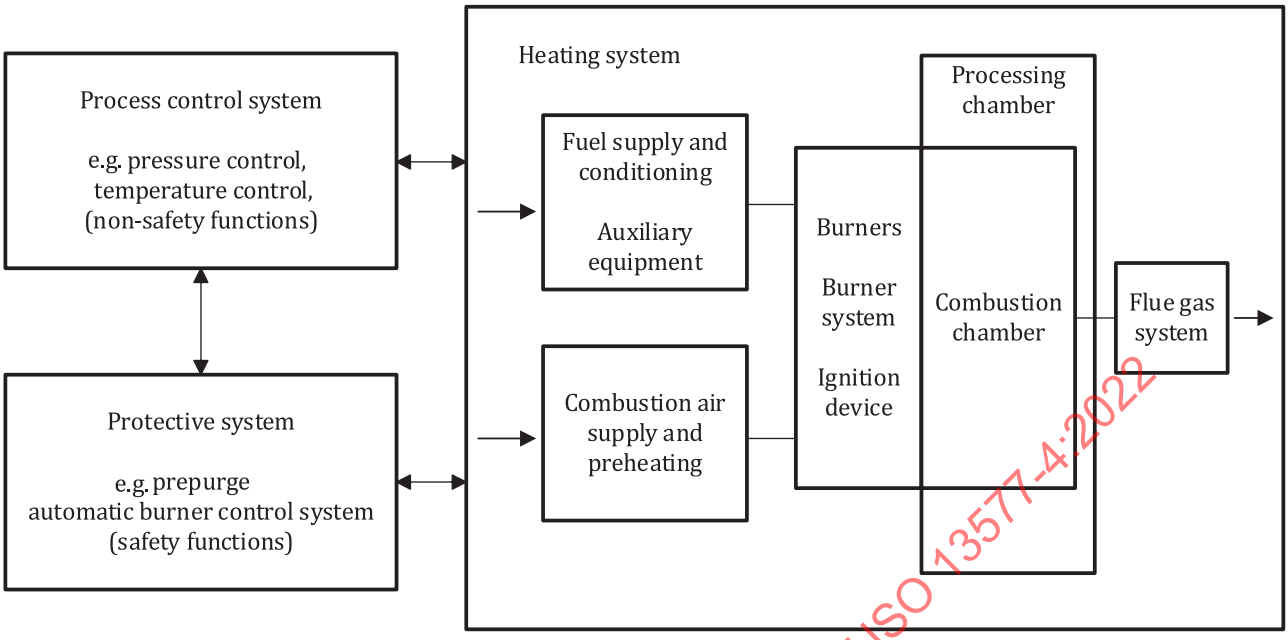


Figure 1 — Block diagram of control and protective systems

An appropriate group of techniques and measures shall be used that are designed to prevent the introduction of systematic faults during the design and development of the hardware and software of the protective system (see Annex A).

Failure due to short circuit in external wiring shall be avoided (see B.5 and Figure B.10).

The wiring of safety-relevant sensors and actuators, which are part of a protective system, usually are made in the field, outside of electrical enclosures. Short circuits, cross-circuits and earth faults in that field wiring can cause safety critical faults to the entire protective system. Cable loops for connecting field devices shall be suitably routed and fastened to prevent damage to the cables.

In order to keep the entire protective system in a safe condition, the field wiring of safety-relevant sensors and actuators (e.g. pressure switches, gas valves) shall be protected against mechanical damage (including, e.g. vibration or bending) to prevent short circuits, cross circuits and earth faults.

NOTE 2 A method to protect against short circuits, cross circuits and earth faults is to use cable-ducts, cable trays, or conduits for the field wiring.

If the protective system is operated in non-grounded, insulated mains, an insulation monitoring device shall be foreseen. This isolation monitoring device immediately needs to isolate all poles of the protective system from the mains in the event of the first fault detection.

Requirements for testing and testing intervals for protective systems shall be specified in the instruction handbook. Except as permitted by method D, the testing of all safety functions shall be performed at least annually. Method D shall be used if the testing of all safety functions is performed beyond 1 year.

See Annexes C and D for examples of SIL/PL determinations.

4.2 Requirements for protective systems

4.2.1 Overview of methods

Any one or a combination of the three (3) methods shall be used to implement a protective system for the safety function(s) requirements identified in the ISO 13577 series; however, only one method shall be used for any one specific safety function. The three methods are the following:

— method A as specified in 4.2.2;

— method BC as specified in 4.2.3;

— method D as specified in 4.2.4.

Figure 2 shows the basic configuration of a protective system.

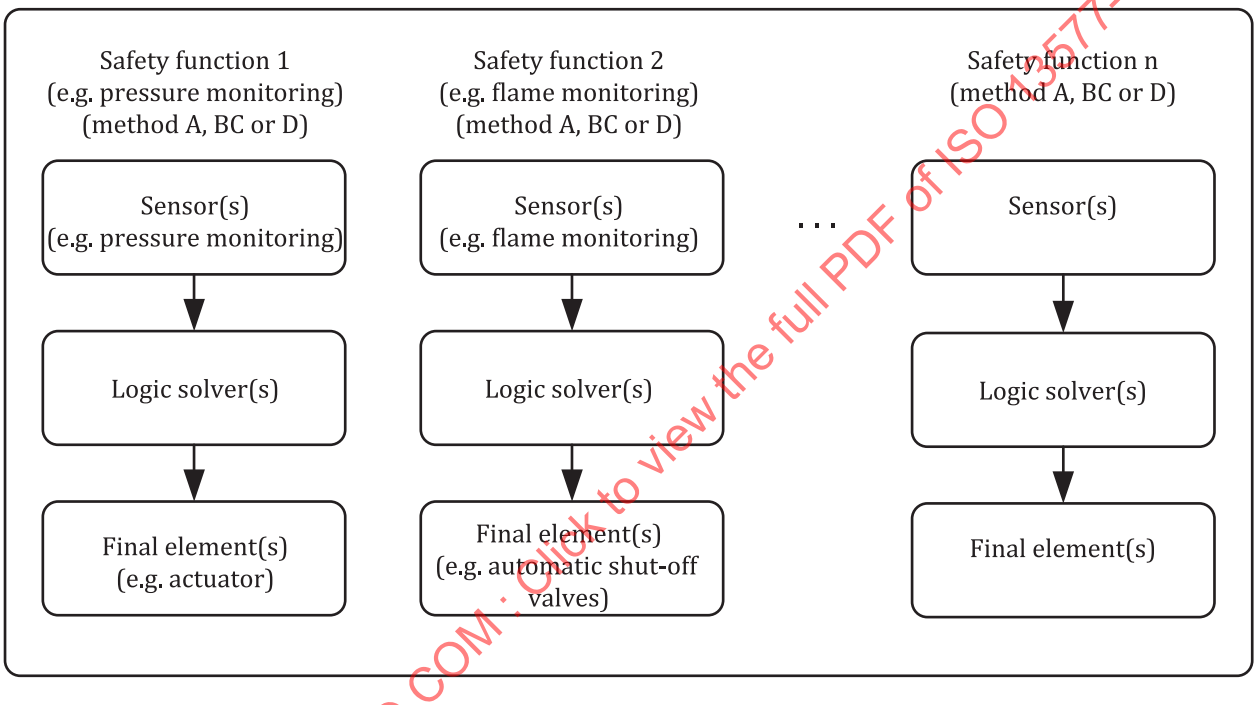


Figure 2 — Basic configuration of a protective system

Figure 3 shows the basic characteristics of each method.

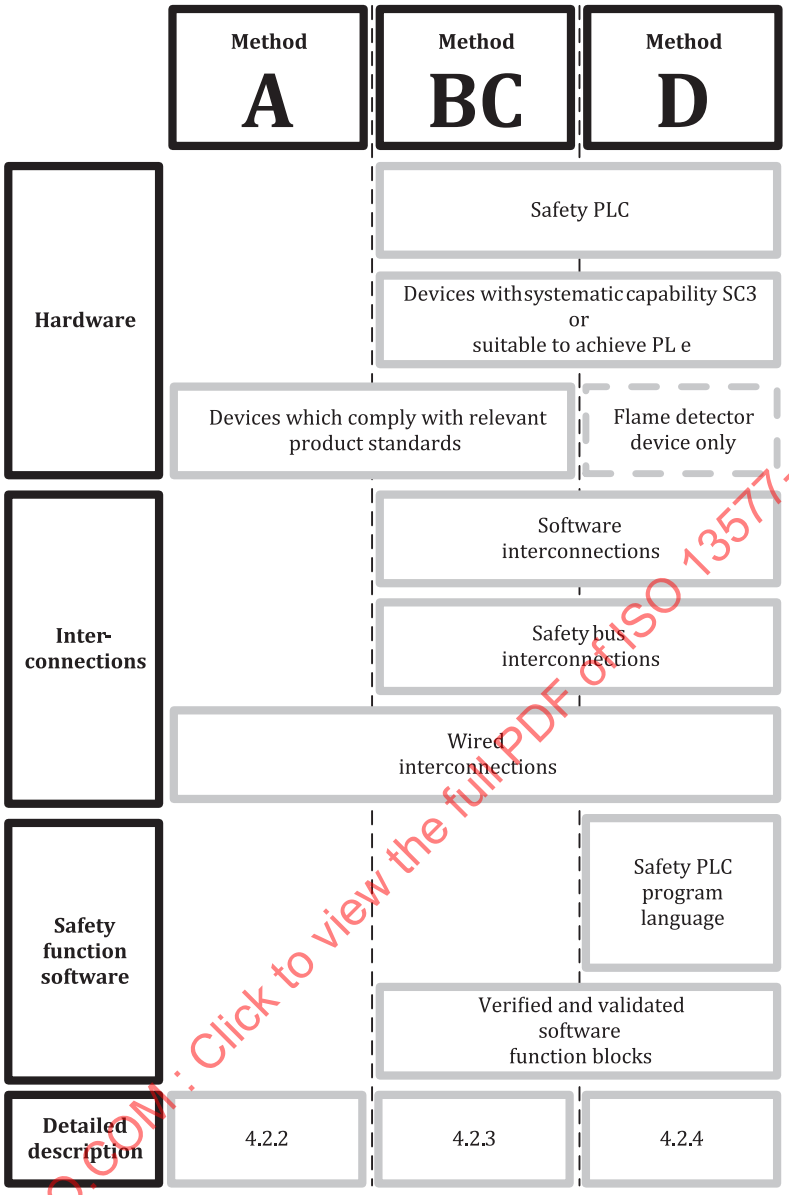


Figure 3 — Method overview

NOTE 1 Software interconnections are links between software function blocks, safety PLC inputs, and safety PLC outputs. These are similar to wired interconnections between devices.

NOTE 2 A safety function software is either a software function block or program to perform safety logic functions (e.g. prepurge, automatic burner control), see 4.2.2.

See Annex E for examples for protective functions of the various methods.

4.2.2 Method A

Method A shall be a wired system in which all devices (i.e. sensors, logic solver, and final elements described in Figure 4) comply with the product standards as specified in the ISO 13577 series.

The requirements of the IEC 61508:2010 series, the IEC 61511:2016 series, IEC 62061:2021, and ISO 13849-1:— are not applicable for this type of protective system.

The following requirements for wiring shall be fulfilled:

a) all logic solvers shall be supplied by the devices and through the direct interconnections between the devices;

b) devices with fixed program language, which meet the relevant product standards, shall be permitted;

c) connections shall not be permitted through data communication buses;

d) wiring of the protective system shall be in accordance with Annex B.

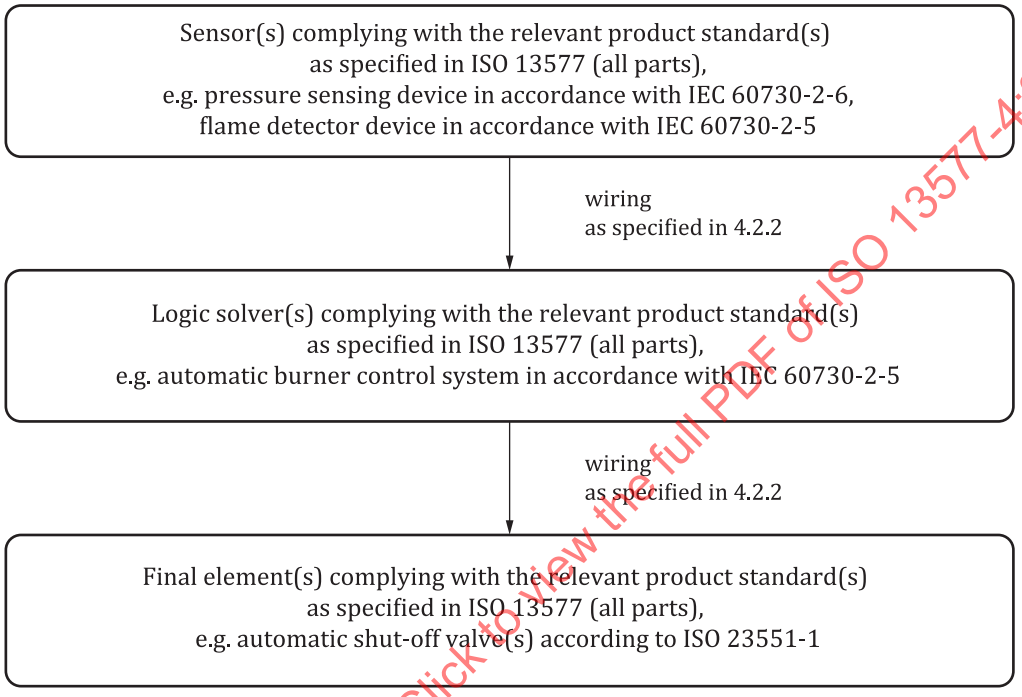


Figure 4 — Hardware configuration of Method A

NOTE The safety devices used in 4.2.2 correspond to specific safety requirements, matched to the field of application and the functional requirements made of these devices, as demanded in the corresponding product standards for safety devices, e.g. automatic burner control systems, valve-proving systems, pressure sensing devices, automatic shut-off valves. Even without additional SIL/PL certification of these safety devices, the safety requirements for use of safety devices are in compliance with relevant product standards. Implementation of a protective system in accordance with 4.2.2 is one of several alternative methods.

4.2.3 Method BC

Method BC shall be a combination of devices meeting the relevant product standards and/or SIL/PL capable devices for which no product standard exists. The use of safety PLCs is optional (see Figure 5).

The following requirements for wiring shall be fulfilled:

a) all logic solvers shall be supplied by the devices and through the direct interconnections between the devices;

b) devices with fixed program language, which meet the relevant product standards, shall be permitted;

c) the interconnections shall be wired, or by safety bus, or by software interconnections;

d) wiring of the protective system shall be in accordance with Annex B.

When using programmable logic solver (e.g. safety PLC), a safety function software shall be verified and validated SIL 3 capable software function blocks (see Figure 5). In addition, the following requirements shall be fulfilled:

i) where a programmable device implements a safety function that is partly or entirely addressed in a relevant product standard, the software function shall be verified and validated with respect to the applicable requirements in the related product standard including but not limited to the sequences and timings of the product standard;

ii) software interconnections in a programmable device shall be verified and documented by a functional test in accordance with the functional safety standards;

iii) software programming languages for PLCs shall be in accordance with IEC 61131-3:2013;

iv) software shall be locked and secured against unauthorized and unintended changes.

NOTE 1 Verification and validations of SIL/PL certification of system software (see IEC 61508-4:2010, 3.2.6 and 3.2.7) and devices is typically carried out by a notified body, accredited national testing laboratory, or by an organization in accordance with ISO/IEC 17025.

Safety functions shall be within a safety-rated device or within an external device covered by the relevant product standard.

For the devices (safety PLC, timers, etc.), which are NOT covered by product standards, the following requirements shall be fulfilled:

1) the devices shall have systematic capability SC 3 (SIL 3 capable) in accordance with the IEC 61508:2010 series, the IEC 61511:2016 series, or IEC 62061:2021, or it shall be suitable to achieve PL e in accordance with ISO 13849-1:—;

2) certification shall apply to the complete device, including the hardware and software.

Devices with less than SIL 3/PL e capability shall be permitted provided the SIL/PL requirements for the loop (safety function) are determined based on the risk assessment. The systematic capability of the devices shall conform to the determined SIL/PL as a minimum.

When the SIL of a device is determined based on proven in use, the requirements in the IEC 61508:2010 series shall be adhered to and required documentation be provided in the final assembly documentation. These procedures shall be accepted by the end user.

When the PL is determined by well-tried components, the requirements in ISO 13849-1:— shall be followed.

All requirements in the instructions or safety manual for the device shall be adhered to such as the proof test interval.

NOTE 2 Annex C contains examples of determining SIL/PL.

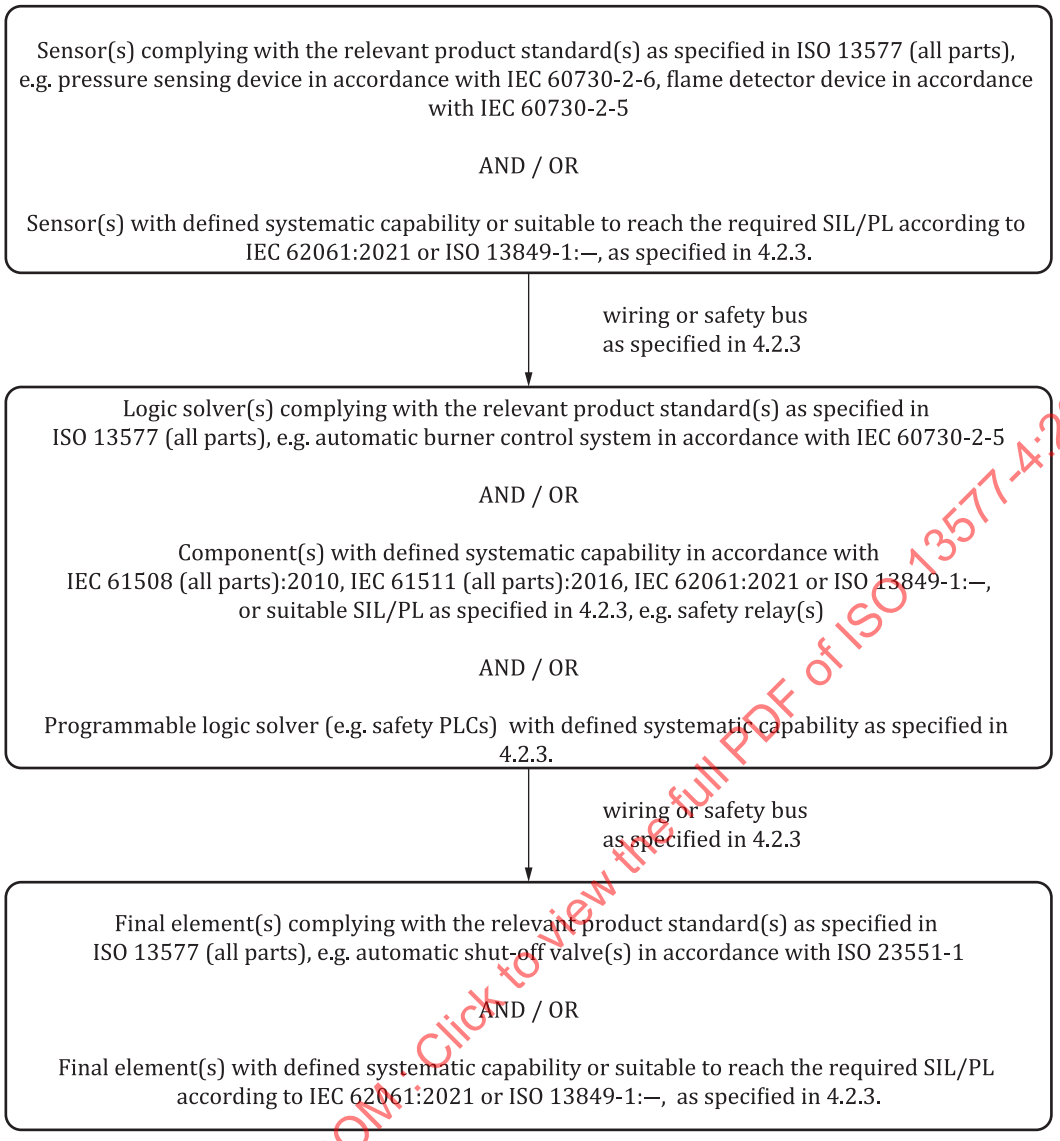


Figure 5 — Hardware configuration of Method BC

4.2.3.1 Requirements for application software of programmable logic solvers

Application software shall be developed in accordance with the methods of functional safety of programmable electronic safety-related systems, defined in the requirements of IEC 61508:2010 series, the IEC 61511:2016 series, IEC 62061:2021, ISO 13849-1:— or Annex F.

NOTE Annex F provides criteria for applications based on the IEC 61508:2010 series.

Manufacturer's instructions for the device shall identify any applicable requirements contained in IEC 61508-3:2010, if software alterations are initiated by the end user.

4.2.4 Method D

Method D shall be in accordance with the full requirements of functional safety standards the IEC 61508:2010 series, the IEC 61511:2016 series, IEC 62061:2021, or ISO 13849-1:— (see Figure 6).

NOTE 1 See Annex D for the method in accordance with the IEC 61511:2016 series.

NOTE 2 See Annex D for one method of hazard and risk assessment in accordance with the IEC 61511:2016 series. The application of other methods according to this document are possible. C.2.2 contains an example for determining SIL in accordance with this document.

Method D shall also fulfil the following requirements:

a) the flame detector device shall comply with IEC 60730-2-5:2013+AMD1:2017+AMD2:2020 CSV;

b) all requirements of the PLC and all safety devices shall be used in accordance with manufacturer's instructions and product safety manual;

c) each functional safety requirement, as identified in the ISO 13577 series, shall be evaluated for its need in accordance with the functional safety standards and implemented with the required SIL/PL for each function. Safety functions of the safety-related system, such as automatic burner control system, valve proving, air/fuel ratio control, etc. shall fulfil the intent of the safety requirements in the relevant product standards;

NOTE 3 A risk assessment in method D can take precedence over the safety requirements in the ISO 13577 series. By nature of the risk assessment under method D, the overall safety is not reduced and meets or exceeds the intended requirements of the ISO 13577 series.

d) the interconnections shall be wired, or by safety bus, or by software interconnections;

e) wiring of the protective system shall be in accordance with Annex B.

NOTE 4 Verification and validations of SIL/PL is typically carried out using an independent checking process similar to 3rd party verification.

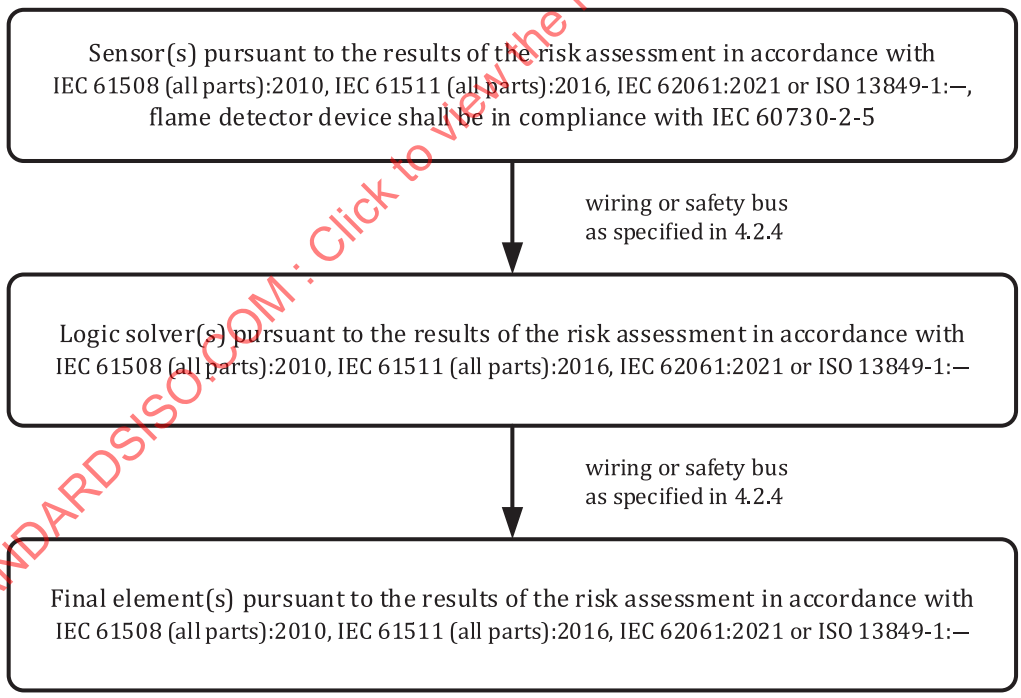


Figure 6 — Hardware configuration of Method D

4.3 Fault assessment for the wired section of protective systems

The protective system shall be designed such that the devices required in the ISO 13577 series shall be used as follows.

a) When relays are used in safety functions, the contacts shall be supervised and mechanically linked, and the current applied to all contacts shall be a maximum of 60 % of the contacts' rating. Control relays for safety shall be in accordance with IEC 60947-5-1:2016 or the requested SIL/PL

requirement. Power relays for safety with or without mirror contacts shall be in accordance with IEC 60947-4-1:2018.

b) The device shall be wired in accordance with the manufacturer's instructions.

c) For method BC, when timers not complying with the relevant product standards as specified in the ISO 13577 series are used in safety functions, timers shall have a systematic capability of SC 3 (SIL 3 capable). Setting of adjustable timers shall be locked or sealed.

d) Overcurrent protection shall be provided to limit current in the safety circuit to below 60 % of the lowest device contact rating.

Additional requirements are given in Annex B.

4.4 Failure of utilities

Loss of utilities (e.g. electrical power, instrument air) to the TPE shall result in safe state (e.g. lock-out). Any restart shall be initiated by manual intervention only. The start-up and ignition sequence shall apply (see ISO 13577-2: —[3], 4.11).

4.5 Reset

Unless permitted by Method D on devices performing a safety function, reset after lock-out shall be triggered manually after remedying the fault (see ISO 13574:2015, 2.107).

The reset shall be implemented as a safety function, it shall comply with ISO 13849-1:—, 5.2.3.2, and it shall not override a safety function.

The design shall incorporate means to prevent unintended and permanent resets.

The design shall incorporate means to prevent unintended start of the TPE.

The instruction handbook shall include a requirement that the operator ensures safe operation prior to initiating a reset.

The maximum number of resets within a defined time span shall be limited and specified, based on the risk assessment, and shall be included in the instruction handbook.

When the manual reset is initiated, direct or camera view of the TPE shall be required. Safe operation shall be ensured from the reset action, and the actual status and relevant information of the process under control shall be verified to the operator.

5 Information for use

Documentation detailing the protective measures and operation shall be included in the equipment documentation.

3) Second edition under preparation. Stage at the time of publication: ISO/FDIS 13577-2:2022.

Annex A
(informative)

Explanation of techniques and measures for avoiding systematic faults

A.1 General

Random faults have physical causes (e.g. temperature extremes, corrosion, wear) and statistical information can be used for a risk analysis. However, systematic faults originate from human errors in the specification and design of the protective system. Systematic faults can be hidden until specific conditions occur and might not be discovered for long periods of time. These specific conditions will cause all equipment that was produced from that system to fail in the same manner. Consequently, it is very important to guard against systematic faults from the beginning stages of a project.

A.2 Competency

Because systematic faults are human in nature, the people and their organization involved in the design and development of protective systems need to be competent for the particular activities for which they are responsible. Each person, department, organization, or other unit needs to be identified and informed of the responsibilities assigned to them (including, where relevant, licensing authorities or safety regulatory bodies). The following items need to be addressed in determining competency for protective system design:

a) engineering knowledge, training, and experience appropriate to:
   1) the process application,
   2) the applicable technology used (e.g. electrical, electronic, programming), and
   3) the sensors and final elements;
b) safety engineering knowledge (e.g. process safety analysis);
c) knowledge of the legal and regulatory functional safety requirements;
d) adequate management and leadership skills appropriate to their role in the design;
e) understanding of the potential consequence of an event;
f) suitability to the novelty and complexity of the application and the technology.

Additional information on competency can be found in IEC 61511-1:2016.

A.3 Avoidance of systematic faults

The following provide a summary of typical activities needed for avoidance of systematic faults during the design stage. More details can be found in IEC 61508-2:2010.

Choose a design method with features that facilitate the following:

a) transparency, modularity, and other features that control complexity;

b) clear and precise expression of:

- functionality,
- subsystem and element interfaces,
- sequencing and time-related information, and
- concurrency and synchronization;

c) clear and precise documentation and communication of information;

d) verification and validation.

Use design features that make the protective system tolerant against systematic faults, random faults, and residual design faults in the hardware, software, and data communication process.

During the design, distinguish and identify those activities that can be carried out at the development premises from those that require access to the user's site.

Formalize maintenance requirements during the design stage to ensure that the safety integrity requirements of the protective systems continue to be met throughout their lifecycles.

Take into account human capabilities and limitations and the actions assigned to operators and maintenance staff, including their likely level of training or awareness.

Design the protective system integration tests and establish the test plan documentation, including the following:

i) the types of tests to be performed and procedures to be followed;

ii) the test environment, tools, configuration, and programs;

iii) the pass/fail criteria.

Where applicable, use automatic testing tools and integrated development tools.

Annex B
(normative)

Wiring of protective systems

B.1 General

Electrical installation and equipment shall comply with IEC 60204-1:2016.

This annex describes how to wire the protective system so as not to reduce the level of safety.

This annex applies to the wiring within the logic solver, and the wiring between the logic solver and the devices that directly or indirectly control the final elements. Moreover, it applies to the field wiring among devices like sensors, interlocks, actuators, final elements, flame detector, igniter, etc.

To maintain the level of safety of the wired protective system, techniques shall be applied to avoid or prevent the introduction of systematic faults during design and development and to apply design features (e.g. self-checking, redundancy) to control both random and systematic faults during operation.

The fault assessment in Figure B.1 shall be applied for the design, fault analysis, and proof of safety.

NOTE Based on the application of Figure B.1, a hazardous situation caused by a single fault can be excluded.

B.2 Protection against faults of the protective system

The protective system shall be designed such that:

a) faults, which could impair the effectiveness of the protective system, shall be minimized by fault-avoidance techniques, such as shown by the examples in Figures B.2 to B.8 or

   NOTE 1 Examples of IMPROPER wiring are shown in Figures B.10 to B.14.

b) in the event of internal faults (e.g. welded relay, incorrect placement of wiring, internal temperature too high) or the occurrence of external influences (e.g. EMC, vibration, temperature too high, dust, lightning), the protective system shall:

   1) not be compromised, or

   2) keep the thermal processing equipment in a safe state or bring it to a safe state (by fault control techniques).

The simultaneous occurrence of two independent faults in different devices need not be taken into account (e.g. two relays fail simultaneously without a common cause).

The combination of a second fault with an undetected first fault shall be taken into account in accordance with Figure B.1. Any faults arising from a first fault (consecutive faults) shall be considered together with this first fault (see Figure B.14).

For systems for non-permanent operation, if a fault is detected at start-up, operation shall not be permitted.

For systems for permanent operation, a second fault is considered to occur 24 h after the first fault (e.g. if the fault is detected during operation, operation shall not be permitted for longer than 24 h after the first fault is detected).

NOTE 2 24 h is an indication of the mean time to restoration (MTTR). Please refer to IEC 61511-1:2016.

B.3 Measures to avoid faults

During development, organizational and design precautions shall be taken to avoid faults, including but not limited to:

a) definition of a project-specific production sequence plan, including but not limited to:

   1) specifications,

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

   3) test plan;

b) segregation of safety-related and non-safety-related functions of devices; and

c) functions and interconnections shall be verified by test.

Particular attention shall be paid to fault avoidance precautions in the case of application-specific integrated circuits.

NOTE See Annex A for techniques and measures for avoidance of systematic faults.

B.4 Hardware design

B.4.1 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 protective functions.

b) The required functions, the 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.

B.4.2 Wired section of the protective system

The wired section of protective system shall be constructed such that the fault assessment according to Figure B.1 results in termination.

Fault assessment for the protective system according to Figure B.1 shall consider failure of auxiliary power and break of connecting lines.

NOTE 1 If certain devices affected by such failures achieve a safe status (e.g. closed-circuit operation in binary circuits), a single-channel design of the relevant parts can 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, normally energized (e.g. closed-circuit operation in binary circuits), would be provided in order to achieve the effectiveness of the protective system (including all pneumatic, hydraulic, and mechanical final elements) for this function.

In the case of output circuits, at least two monitored disconnecting devices, i.e. contactors or relays, shall be provided to obtain safety shutdown of the entire fuel supply.

Reed relays shall not be used for any protective functions.

NOTE 2 Hardware diversity is achieved by different types of construction of electro-mechanical switching devices, for instance, if switching devices of different construction or design are used. Diverse functionality is achieved by closed-circuit arrangement and open-circuit arrangement.

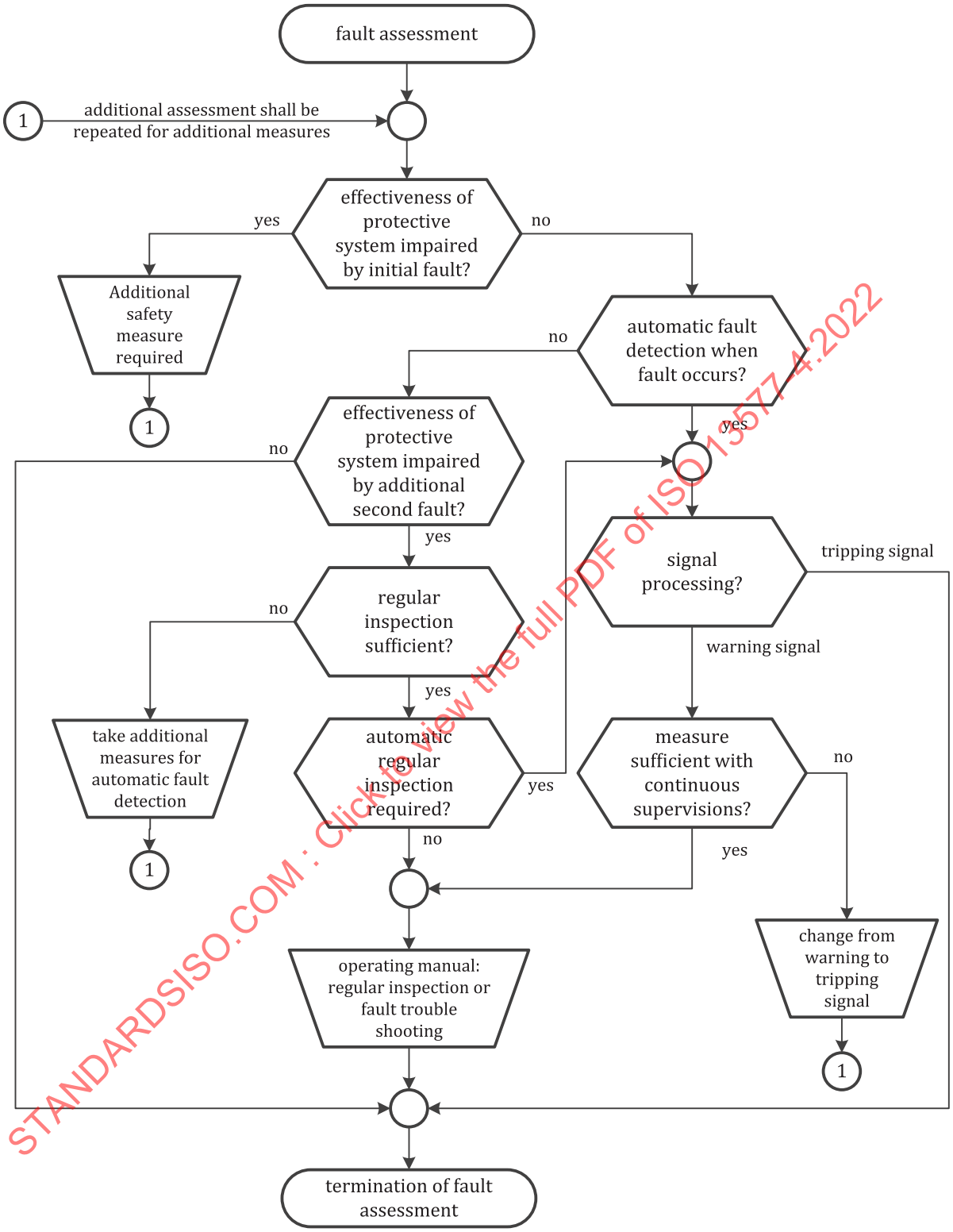


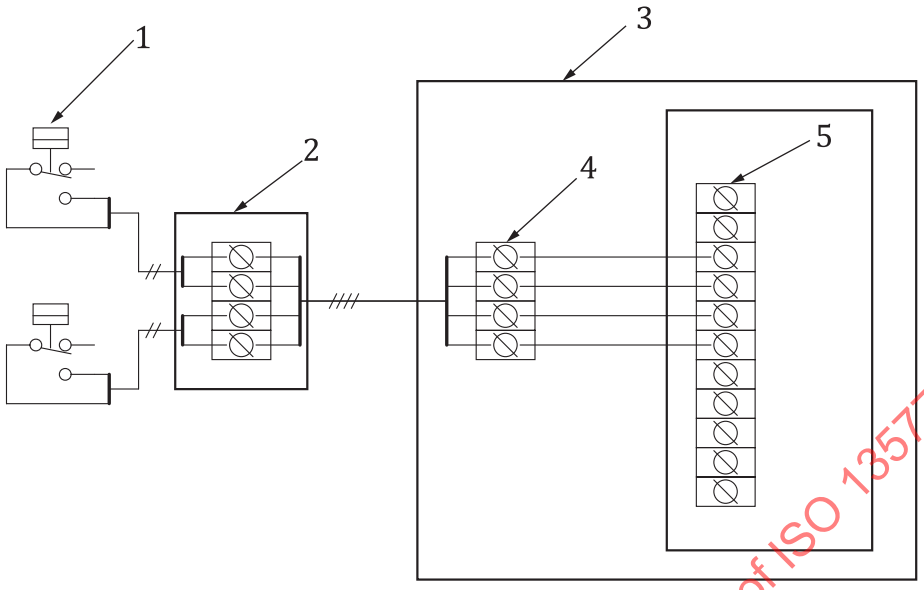
Figure B.1 — Fault assessment for the wired section of a protective system

B.5 Proper input wiring

This clause provides examples of techniques for avoiding failures from external wiring.

Figure B.2 shows a technique that can provide a sufficient level of protection for the safety function when used with protective system methods A, BC, or D. All conductors are brought back to the main

enclosure through cable ducts or conduits, which provide sufficient protection from mechanical and thermal damage. In addition, the protective system device accepts each conductor from the sensors.

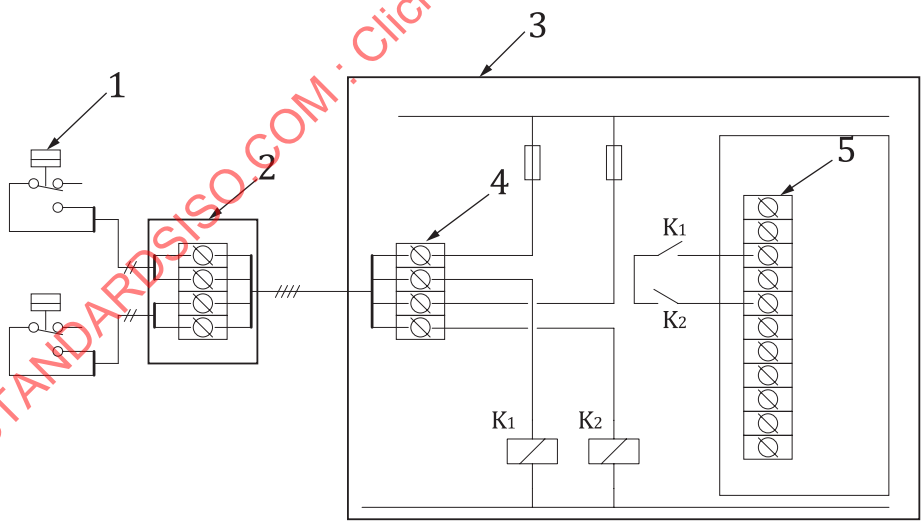


Key

1	digital sensor (e.g. pressure sensing device)	4	enclosure terminals
2	field terminal box	5	digital logic terminals
3	enclosure with logic		

Figure B.2 — Protected wiring

Figure B.3 shows a slight variation, needed in case the logic solver accepts only one digital input.



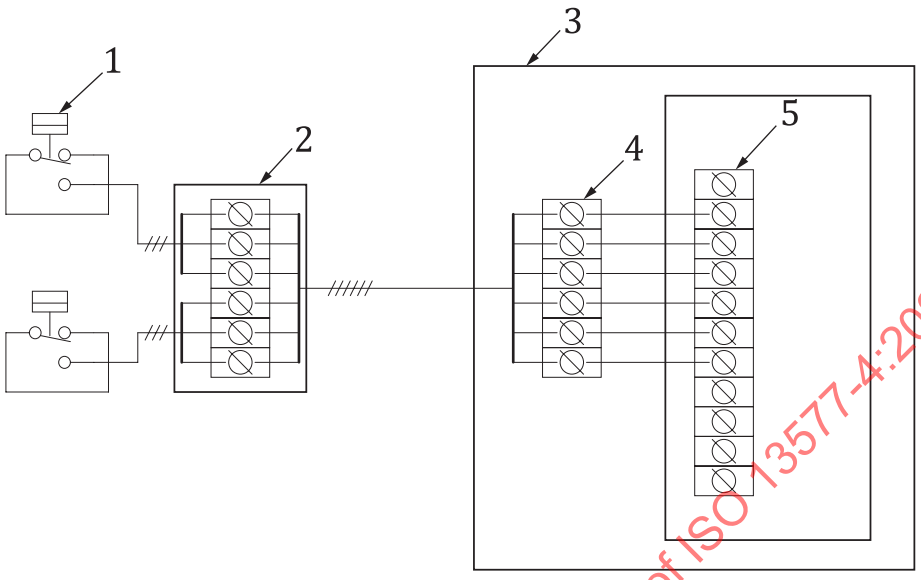
Key

1	digital sensor (e.g. pressure sensing device)	4	enclosure terminals
2	field terminal box	5	digital logic terminals
3	enclosure with logic	K_1, K_2	auxiliary relays (see Figure B.9)

Figure B.3 — Protected wiring with auxiliary relays

Figure B.4 shows a technique where both states of each sensor switch (1 NO and 1 NC contact for each sensor) are monitored by the protective system, and whose logic solver detects the improper condition

caused by a short circuit in the field wiring. This technique is suitable when using any of the protective system methods A, BC, or D.

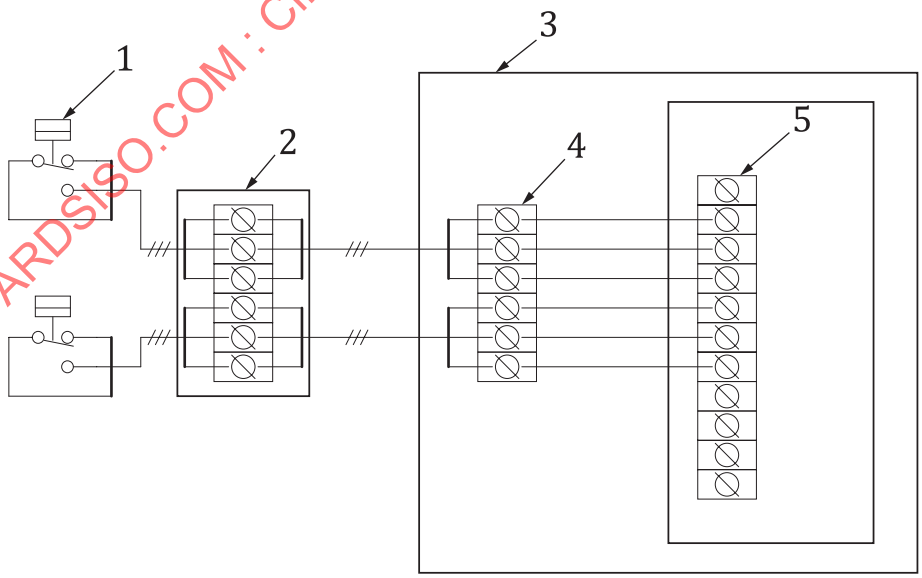


Key

1 digital sensor (e.g. pressure sensing device)
2 field terminal box
3 enclosure with logic
4 enclosure terminals
5 digital logic terminals

Figure B.4 — Supervision of both states

Figure B.5 shows a variation of Figure B.4, whereby the 6-conductor single cable can be replaced with two 3-conductor cables.

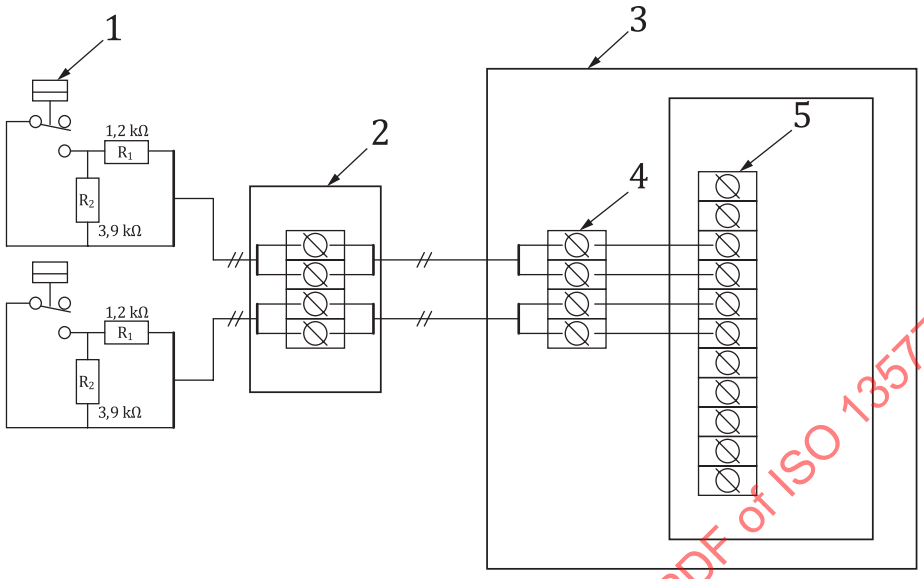


Key

1 digital sensor (e.g. pressure sensing device)
2 field terminal box
3 enclosure with logic
4 enclosure terminals
5 digital logic terminals

Figure B.5 — Supervision of both states, multiple cables

Figure B.6 shows a technique using analogue signals for the switching states and the protective system logic solver detects the improper condition caused by a short circuit in the field wiring (analogue level is out of the acceptable bands for either the high or low state). This technique is suitable when using method BC or D.



Key

1	digital sensor (e.g. pressure sensing device)	5	analog logic terminals
2	field terminal box	R_1	resistor 1 (1,2 kΩ)
3	enclosure with logic	R_2	resistor 2 (3,9 kΩ)
4	enclosure terminals		

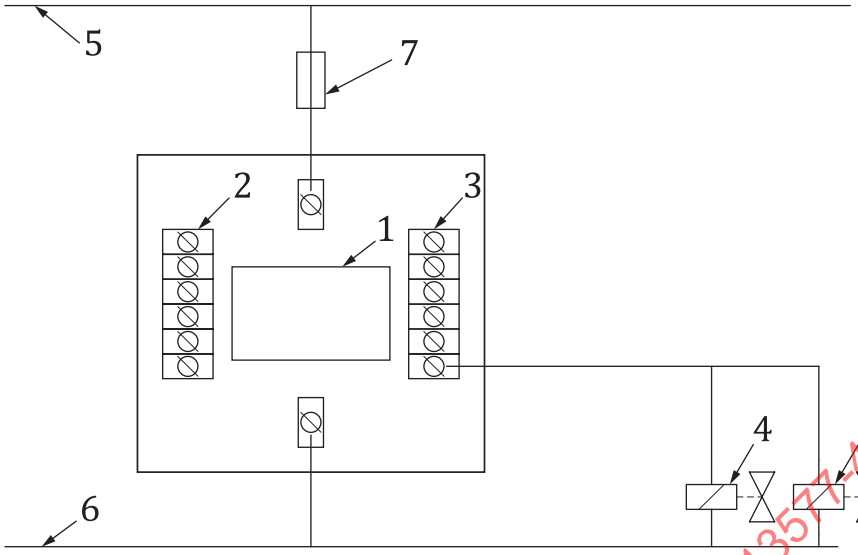
The input card should be capable of detecting open and short circuit.

NOTE Values identified in the figure are examples for 4 mA to 20 mA only.

Figure B.6 — Supervision by analogue value

B.6 Proper output wiring

Figure B.7 shows how to wire two solenoid valves in case of simple automatic electrical burner control system applications. This technique is only suitable when using protective system method A.



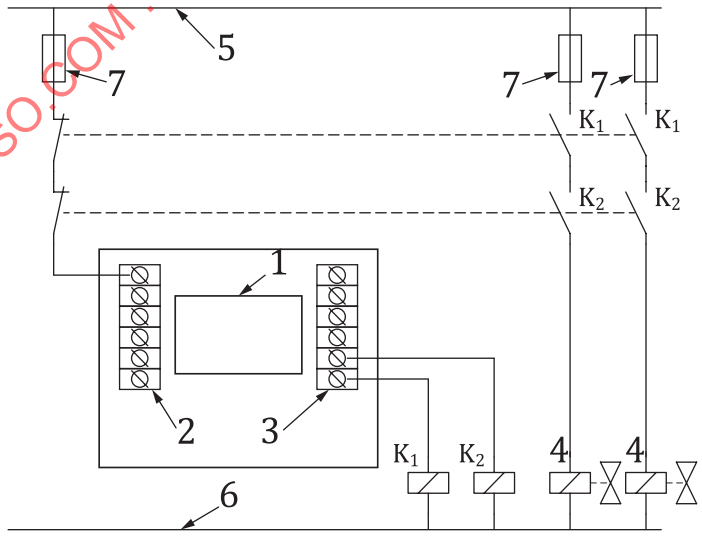
Key

1	automatic electrical burner control system	5	supply voltage
2	safe input	6	neutral
3	safe output	7	fuse
4	fuel valves		

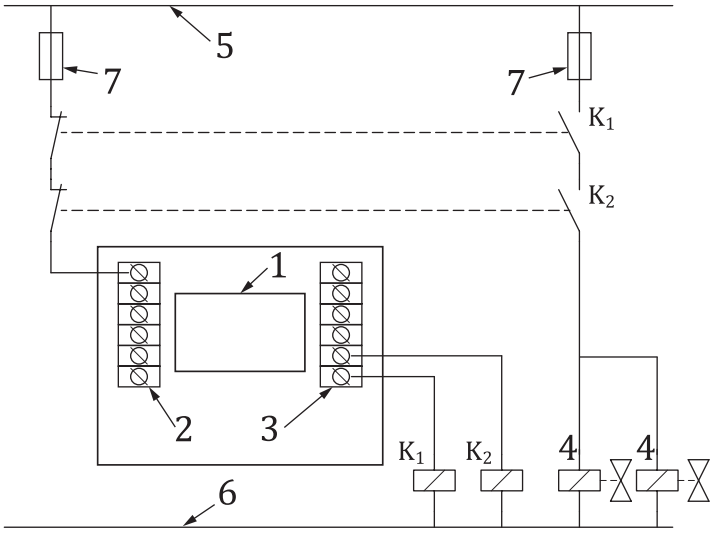
NOTE This figure shows safe output with valve redundancy. Diagnostics can be achieved by flame detection (input signal). In other terms, once the system is shut down, the automatic electrical burner control system detects the absence of the flame.

Figure B.7 — Example of simple automatic electrical burner control system application

Figure B.8 shows wiring in case relays shall be used to power the solenoid valves. This technique is suitable when using protective system methods A, BC, or D.



or



Key

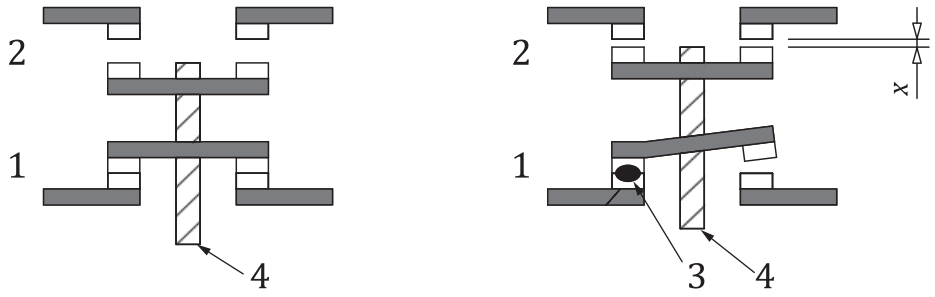
1	logic solver(s)	6	neutral
2	safe input	7	fuse
3	safe output	K_1	relay 1
4	fuel valves	K_2	relay 2
5	supply voltage		

NOTE 1 Relay failures are detected, therefore failures do not accumulate.

NOTE 2 For requirements for relays, see 4.3 a). See also Figure B.9 for basic configuration of relays used in safety circuits.

Figure B.8 — Example of fault avoidance

Figure B.9 shows an example of mechanically linked (IEC 60947-5-1:2016) construction for relay contacts.



Key

1 normally closed contacts
2 normally open contacts
3 welded contact (fault)
4 mechanically linked construction
x minimum distance

Relays used in safety circuits with feedback of the relay position shall be with mechanically linked contacts.

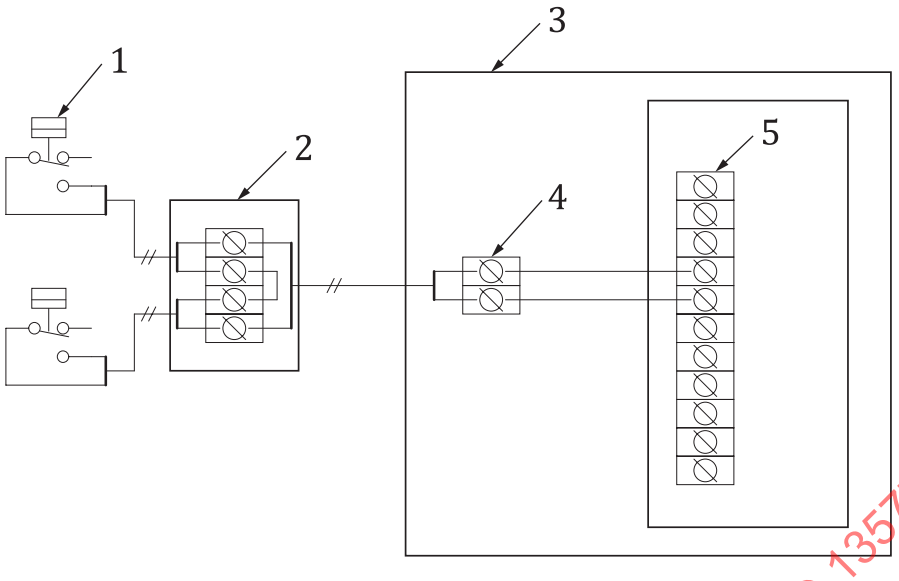
For power relays, mirror contacts shall only be used as feedback of the position of main contacts.

NOTE By design of the mechanical linkage and minimum distance, the normally open contacts remain open when the relay coil is energized and a normally closed contact has welded. Similarly, a fault with welding of a normally open contact causes the normally closed contacts to remain open when the relay coil is de-energized.

Figure B.9 — Example of relay with mechanically linked contacts

B.7 Prohibited input and output wiring

Figure B.10 shows an example of possible short circuit between the field terminal box and enclosure terminals, which would defeat the protective system. For normal safety function, an open state of the pressure switch contacts would cause the logic solver to perform an action through the final element to bring the system to a safe state. With a short circuit between the field terminal box and enclosure terminals, the open state of either switch is not detected.



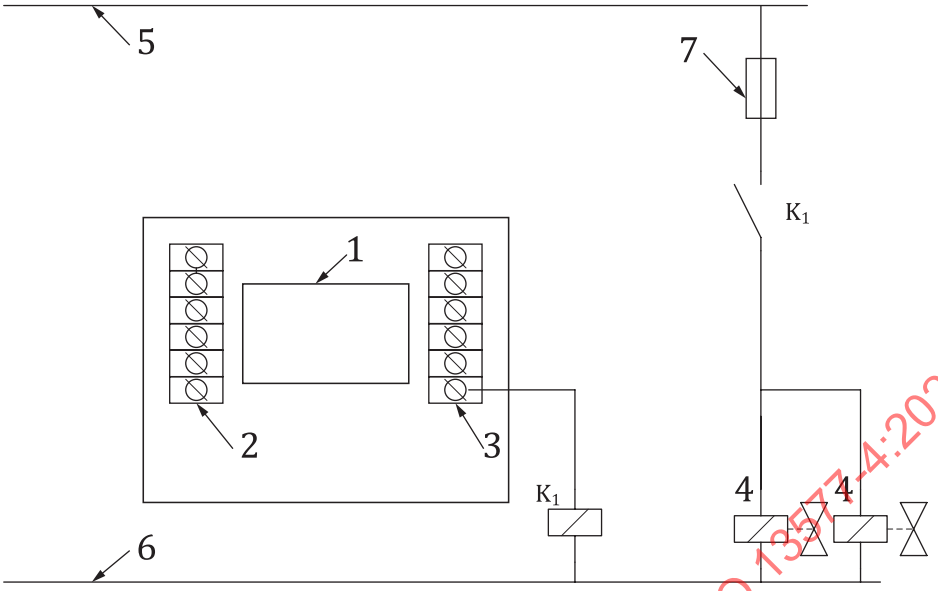
Key

1 digital sensor (e.g. pressure sensing device)
2 field terminal box
3 enclosure with logic
4 enclosure terminals
5 digital logic terminals

CAUTION The external wiring method shown in this diagram shall NOT be used.

Figure B.10 — Prohibited external wiring method

Figures B.11, B12, and B13 show examples of **prohibited** wiring, even when relays as described in Figure B.9 are used.



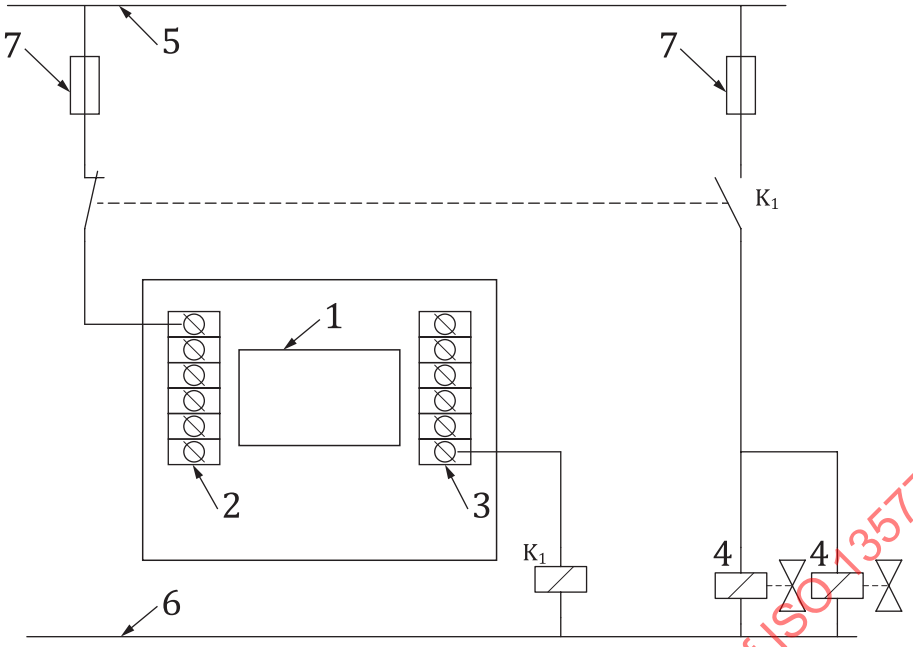
Key

1	logic solver(s)	5	supply voltage
2	safe input	6	neutral
3	safe output	7	fuse
4	fuel valves	K_1	relay 1

CAUTION The external wiring method shown in this diagram shall NOT be used.

NOTE Since only one relay is used, one single failure can result in the loss of the safety function.

Figure B.11 — Example of prohibited wiring



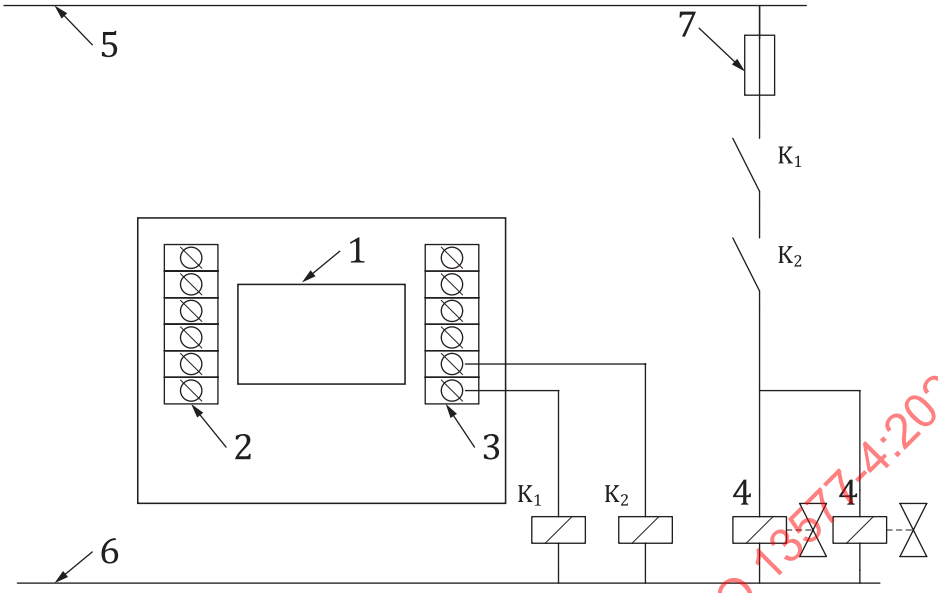
Key

1	logic solver(s)	5	supply voltage
2	safe input	6	neutral
3	safe output	7	fuse
4	fuel valves	K_1	relay 1

CAUTION The external wiring method shown in this diagram shall NOT be used.

NOTE Since only one relay is used, even with its monitoring, one single failure can result in the loss of the safety function.

Figure B.12 — Example of prohibited wiring



Key

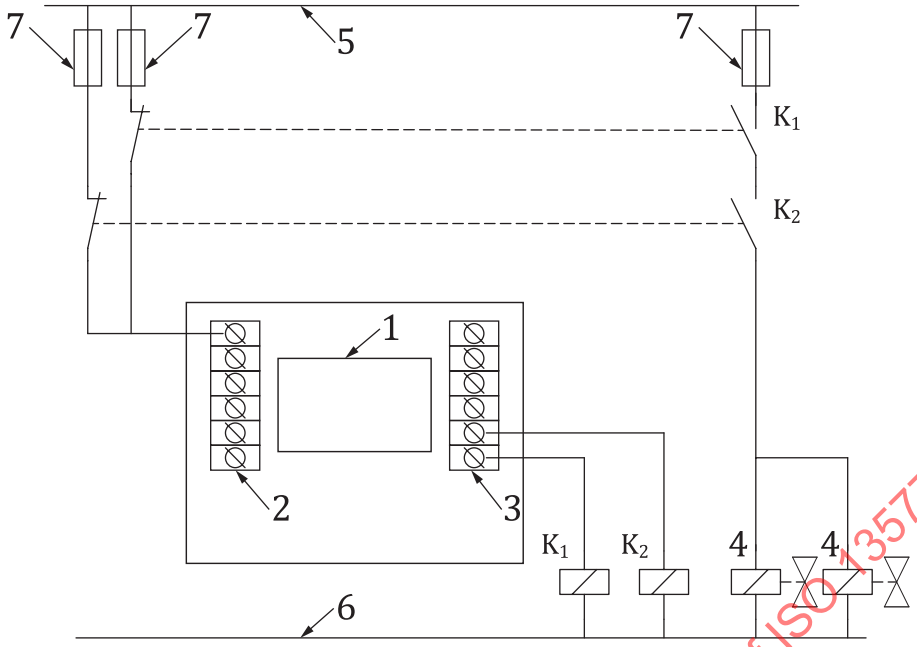
1	logic solver(s)	6	neutral
2	safe input	7	fuse
3	safe output	K_1	relay 1
4	fuel valves	K_2	relay 2
5	supply voltage		

CAUTION The external wiring method shown in this diagram shall NOT be used.

NOTE One single failure avoids the loss of the safety function, but since relay failures are undetected, failures can accumulate and result in the loss of the safety function.

Figure B.13 — Example of prohibited wiring

Figure B.14 shows an example of **prohibited** output wiring. Correct wiring is shown in Figure B.8.



Key

1	logic solver(s)	6	neutral
2	safe input	7	fuse
3	safe output	K_1	relay 1
4	fuel valves	K_2	relay 2
5	supply voltage		

CAUTION The external wiring method shown in this diagram shall NOT be used.

NOTE One single relay failure is not detected, therefore accumulation of failures can result in the loss of the safety function.

Figure B.14 — Example of prohibited wiring of the monitoring relays

Annex C
(informative)

Examples for the determination of safety integrity level (SIL) or performance level (PL) using the risk graph method

C.1 General

The following provides a partial example of the procedures that are used when designing a system for a protective system using method BC when devices do not relate to a product standard and the capability is less than SIL 3/PL e.

Several International Standards can be used for determination of the required SIL/PL. For machinery, IEC 62061:2021 was developed to determine the SIL while the IEC 61511:2016 series was developed to determine the required SIL for process industry. Risk graph methods for determining the safety integrity level SIL are given in both IEC standards (IEC 62061:2021 and the IEC 61511:2016 series). In addition, ISO 13849-1:— covers the determination of a performance level PL and also includes a method to determine PL from SIL (ISO 13849-1:—, Table 3).

A hazard and risk analysis needs to be carried out for each hazard to the industrial furnace and associated processing equipment (TPE). When describing the hazard, the cause of the hazardous situation shall also always be stated. For example, an explosion in the furnace can be brought about by a wide variety of causes such as overheating, excess fuel pressure, insufficient fuel/air ratio, etc. Each of these causes is then assigned at least one safety-related function, which then must reduce the resultant risk.

The required SIL/PL for each safety-related function depends on different parameters:

1) consequences of the hazardous event (parameter Se in accordance with IEC 62061:2021, Annex A, parameter C in accordance with IEC 61511-3:2016); the worst-case scenario shall be taken into account;

2) frequency and duration of the time spent in the hazardous area (parameter Fr in accordance with IEC 62061:2021, Annex A, parameter F in accordance with IEC 61511-3:2016); 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;

3) possibility of preventing or avoiding the hazardous event (parameter Av in accordance with IEC 62061:2021, Annex A, parameter P in accordance with IEC 61511-3: 2016);

4) probability of occurrence of the hazardous event or demand rate (parameter Pr in accordance with IEC 62061:2021, Annex A, parameter W in accordance with IEC 61511-3: 2016).

Parameter Av in accordance with IEC 62061:2021, Annex A and parameter P in accordance with IEC 61511-3:2016 can be estimated by taking into account aspects of the TPE design and its intended application, which can help to avoid or limit the harm from a hazard. These aspects include, for example, the speed of appearance of the hazardous event (sudden, fast, or slow), the spatial possibility to withdraw from the hazard, the nature of the device or system, and the possibility of recognition of a hazard. The lowest value 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.

Parameter Pr in accordance with IEC 62061:2021, Annex A and parameter W in accordance with IEC 61511-3:2016 encompass 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 for avoiding this specific risk, can be taken into account in reducing this parameter.

The results of the SIL/PL determination with rationale and the decisions made shall be documented.

C.2 Examples for the determination of the required SIL/PL

C.2.1 Example 1 – Table C.1

Table C.1 shows a comparison of example of SIL/PL determination under different risk environment in accordance with IEC 62061:2021, Annex A and ISO 13849-1:—, Table 3.

C.2.2 Example 2 – Table C.2

Table C.2 shows an example of SIL determination under different risk environment in accordance with IEC 61511-3:2016.

Table C.1 — Comparison of SIL/PL determination under different risk environment in accordance with IEC 62061:2021 and ISO 13849-1:–, Table 3

Risk assessment and safety measures

Document No.:

Part of:

Project: Example of typical SIL determination

Issued by:

Date:

Revision:

☐ Pre-risk assessment

☐ Intermediate risk assessment

☐ Follow up risk assessment

Black area = Safety measures required

Grey area = Safety measures recommended

Consequences	Severity	Class Cl					Frequency and duration, Fr		Probability of hzd. event, Pr		Avoidance Av	
	Se	3 – 4	5 – 7	8 – 10	11 – 13	14 – 15						
Death, loss of an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	Very high	5		
Permanent, loss of fingers	3		OM	SIL 1	SIL 2	SIL 3	>1 h - ≤d	5	Likely	4		
Reversible, medical attention	2			OM	SIL 1	SIL 2	>1d - ≤ 2 wks	4	Possible	3	Impossible	5
Reversible, first aid	1				OM	SIL 1	>2wks - ≤ 1 yr	3	Rarely	2	Possible	3
							>1 yr	2	Negligible	1	Likely	1

SRCF	**Hazardous event**	**Safety-related control function (SRCF)**	Consequences		Probability of occurrence			Class	Integrity		**Comments**
No.	Description	Description		Se	Fr	Pr	Av	Cl	**SIL**	**PL**	
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.		**4**	3	2	3	**8**	2[a]	**d**	Lower risk environment Minor consequences for few people who have a good chance to escape in time ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown, injuries from hot parts
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.		**4**	5	2	3	**10**	**2**	**d**	Medium risk environment Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown, injuries from hot parts

NOTE For guidance of this risk graph, see C.2.3.

Table C.1 *(continued)*

10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.		**4**	5	3	3	**11**	**3**	**e**	Higher risk environment Major consequences for many people who cannot escape in time. ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown, injuries from hot parts
12	Combustion air pressure/ flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.		**4**	5	2	1	**8**	**2**	**d**	Lower risk environment Minor consequences for few people who have a good chance to escape in time ISO 13577-2: —, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
12	Combustion air pressure/ flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.		**4**	5	2	3	**10**	**2**	**d**	Medium risk environment Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
12	Combustion air pressure/ flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.		**4**	5	3	3	**11**	**3**	**e**	Higher risk environment Major consequences for many people who cannot escape in time ISO 13577-2:—, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
13	Air/gas ratio outside safe operating range	The correct air/gas ratio is controlled by mechanical, pneumatic or electric systems. The electric ratio sensor combined with a logic system shall bring the ratio to a safe level.		**4**	2	3	5	**10**	**2**	**d**	Lower risk environment Minor consequences for few people who have a good chance to escape in time ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning
NOTE For guidance of this risk graph, see C.2.3.											

Table C.1 *(continued)*

13	Air/gas ratio outside safe operating range	The correct air/gas ratio is controlled by mechanical, pneumatic or electric systems. The electric ratio sensor combined with a logic system shall bring the ratio to a safe level.		**4**	5	4	5	**14**	**3**	**e**	Medium risk environment Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning
13	Air/gas ratio outside safe operating range	The correct air/gas ratio is controlled by mechanical, pneumatic or electric systems. The electric ratio sensor combined with a logic system shall bring the ratio to a safe level.		**4**	5	5	5	**15**	**3**	**e**	Higher risk environment Minor consequences for several people who have a reasonable chance to escape in time. ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning

NOTE For guidance of this risk graph, see C.2.3.

Table C.2 — SIL determination under different risk environment in accordance with the IEC 61511-3:2016 series

Project:	Example of typical SIL determination								Process:											
Issued by:									SIF:											
Date:									Plant:											
Revision									Risk:											
Consequence parameter			Risk graph matrix						Occupancy parameter				Avoidance parameter				Demand rate parameter			
									Frequency of human presence in the hazardous zone. Credit for limited occupancy shall not have been taken choosing consequence categories!				Probability of avoiding the hazardous event **if the SIF fails on demand**. Implies **independent** facilities provided to "shut-down" so hazard can be avoided or enable all persons to escape to a safe area. Conditions to be fulfilled: — facilities to alert operator that the SIS has failed; — independent facilities to bring process to safe state; — time between operator alert and hazardous event >1h.				Estimated SIF demand rate			W
			Likelihood sum (F+P+W)														W_9	Often	>1/ year	9
Severity level		C	1-2	3-4	5-6	7-8	9-10	11-12									W_8	Frequent	1/(1-3) years	8
C_F	Catastrophic	F	a	SIL 1	SIL 2	SIL 3	SIL 4	b									W_7	Likely	1/(3-10) years	7
C_E	Extensive	E	OK	a	SIL 1	SIL 2	SIL 3	SIL 4	Exposure rate			F					W_6	Probable	1/(10-30) years	6
C_D	Serious	D	OK	OK	a	SIL 1	SIL 2	SIL 3	F_D	Permanent	100 %	2					W_5	Occasional	1/(30-100) years	5
C_C	Considerable	C	OK	OK	OK	a	SIL 1	SIL 2	F_C	Frequent	10 % –100 %	2	Avoidance probability			P	W_4	Remote	1/(100-300) years	4
C_B	Marginal	B	OK	OK	OK	OK	a	SIL 1	F_B	Occasionally	1 % – 10 %	1	P_B	Avoidance condition not fulfilled		1	W_3	Improbable	1/(300-1 000) years	3
C_A	Negligible	A	OK	OK	OK	OK	OK	a	F_A	Rare	<1 %	0	P_A	All avoidance conditions are fulfilled		0	W_2	Incredible	1/(1 000-10 000) years	2
																	W_1	Inconceivable	1/(10 000-10 000 0) years	1

SIF	Hazardous event	Safety instrumental function (SIF)	Consequences		Influence		Demand	Likelihood	Integrity		Hazard description
No.	Description	Description	Harm	C	F	P	W	Sum	SIL	SIL	and comments
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.	H	D	1	0	6	7	1	1	Major consequences for few people who cannot escape in time ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown injuries from hot parts
			E	B	1	0		7	—		
			E	B				7	1		

NOTE For guidance of this risk graph, see C.2.4.

Table C.2 *(continued)*

10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.	H	D	2	1	6	9	2	2	Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown injuries from hot parts
			E	B	1	1		8	—		
			F	D				8	2		
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature-sensing control in combination with a logic system is monitoring the process temperature. If the temperature rises above the safe level, it shall be brought into a safe state.	H	D	2	1	7	10	2	2	Major consequences for many people who cannot escape in time ISO 13577-2:—, 4.3.6/4.5.8 Hazard: fire, mechanical breakdown, injuries from hot parts
			E	B	1	1		9	a		
			F	D				9	2		
12	Combustion pressure/flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.	H	D	1	0	6	7	1	2	Minor consequences for few people who have a good chance to escape in time ISO 13577-2:—, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	0		7	—		
			E	E				7	2		
12	Combustion air pressure/flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.	H	D	2	1	6	9	2	2	Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	1		8	—		
			F	E				8	2		
12	Combustion air pressure/flow too low	Pressure-sensing device, pressure transmitter or flow sensing device is monitoring the air pressure/flow, and in combination with the logic circuit brings the plant to a safe state if the pressure/flow decreases below a safe level.	H	E	2	1	6	9	3	3	Major consequences for many people who cannot escape in time ISO 13577-2:—, 4.6.2 Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	1		8	—		
			F	E				8	2		
13	Air/gas ratio outside safe operating range	Air/gas ratio outside safe operating range	H	D	1	0	7	8	1	2	Minor consequences for few people who have a good chance to escape in time ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning
			E	B	1	0		8	—		
			F	E				8	2		
13	Air/gas ratio outside safe operating range	The correct air/gas ratio is controlled by mechanical, pneumatic or electric systems. The electric ratio sensor combined with a logic system shall bring the ratio to a safe level.	H	D	2	1	7	10	2	3	Minor consequences for several people who have a reasonable chance to escape in time ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning
			E	B	1	1		9	a		
			F	E				9	3		
NOTE For guidance of this risk graph, see C.2.4.											

Table C.2 *(continued)*

13	Air/gas ratio outside safe operating range	The correct air/gas ratio is controlled by mechanical, pneumatic or electric systems. The electric ratio sensor combined with a logic system shall bring the ratio to a safe level.	H	E	2	1		7	10	3	3	Major consequences for many people who cannot escape in time ISO 13577-2:—, 4.6.3 Hazard: explosion, fire, poisoning
			E	B	1	1			9	a		
			F	E					9	3		
NOTE For guidance of this risk graph, see C.2.4.													

C.2.3 Risk estimation and SIL assignment in accordance with IEC 62061:2021, Annex A (i.e. Table C.1)

C.2.3.1 Hazard identification/indication

Indicate the hazards, including those from reasonable foreseeable misuse, whose risks are to be reduced by implementing an SRCF. List them in the hazard column in Table C.7.

C.2.3.2 Risk estimation

Risk estimation should be carried out for each hazard by determining the risk parameters that, as shown in Figure C.1, should be derived from the following:

— severity of harm, Se;

— probability of occurrence of that harm, which is a function of:

a) frequency and duration of the exposure of persons to the hazard, Fr,

b) probability of occurrence of a hazardous event, Pr, and

c) possibilities to avoid or limit the harm, Av.

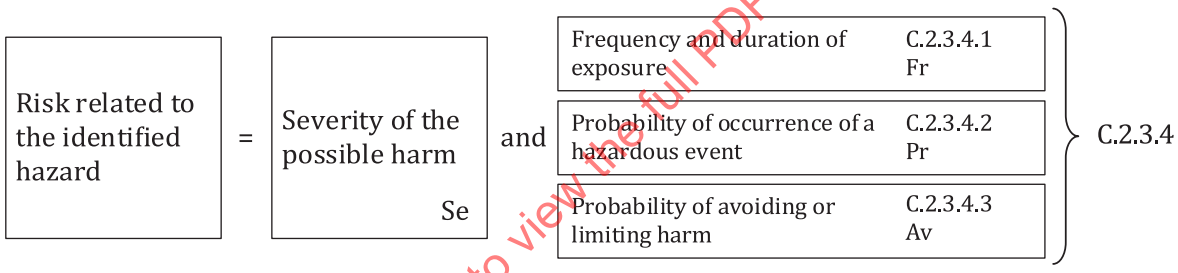


Figure C.1 — Parameters used in risk estimation

The estimates entered into Table C.7 should normally be based on worst-case considerations for the SRCF. However, in a situation where, for example, an irreversible injury is possible but at a significantly lower probability than a reversible one, then each severity level should have a separate line on the table. It might be the case that a different SRCF is implemented for each line. If one SRCF is implemented to cover both lines, then the highest target SIL requirement should be used.

C.2.3.3 Severity (Se)

Severity of injuries or damage to health can be estimated by taking into account reversible injuries, irreversible injuries, and death. Choose the appropriate value of severity from Table C.3 based on the consequences of an injury, where:

4 means a fatal or a significant irreversible injury such that it will be very difficult to continue the same work after healing, if at all;

3 means a major or irreversible injury in such a way that it can be possible to continue the same work after healing. It can also include a severe major but reversible injury such as broken limbs;

2 means a reversible injury, including severe lacerations, stabbing, and severe bruises that requires attention from a medical practitioner;

1 means a minor injury including scratches and minor bruises that require attention by first aid.

Select the appropriate row for consequences (Se) of Table C.3. Insert the appropriate number under the Se column in Table C.7.

Table C.3 — Severity level in consequence – Health hazard (H)

Consequences	Severity (Se)
Irreversible: death, losing an eye or arm	4
Irreversible: broken limb(s), losing a finger(s)	3
Reversible: requiring attention from a medical practitioner	2
Reversible: requiring first aid	1

C.2.3.4 Probability of occurrence of harm

Each of the three parameters of probability of occurrence of harm (i.e. Fr, Pr, and Av) should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that SRCF(s) are not incorrectly assigned a lower SIL than is necessary. Generally, the use of a form of task-based analysis is strongly recommended to ensure that proper consideration is given to estimation of the probability of occurrence of harm.

C.2.3.4.1 Frequency and duration of exposure (Fr)

Consider the following aspects to determine the level of exposure:

— need for access to the danger zone based on all modes of use, for example, normal operation, maintenance;

— nature of access, for example, manual feed of material, setting.

It should then be possible to estimate the average interval between exposures and therefore the average frequency of access.

It should also be possible to foresee the duration, for example, if it will be longer than 10 min. Where the duration is shorter than 10 min, the value can be decreased to the next level. This does not apply to frequency of exposure ≤1 h, which should not be decreased at any time.

The duration is related to the performance of activities that are carried out under the protection of the SRCF. The requirements of IEC 60204-1:2016 and ISO 14118 with regard to power isolation and energy dissipation should be applied for major interventions.

This factor does not include consideration of the failure of the SRCF.

Select the appropriate row for frequency and duration of exposure (Fr) of Table C.4. Insert the appropriate number under the Fr column in Table C.7.

Table C.4 — Frequency and duration of exposure (Fr) classification

Frequency and duration of exposure (Fr)	
Frequency of exposure	**Duration >10 min.**
≤1 h	5
>1 h to ≤1 day	5
> 1 day to ≤2 weeks	4
>2 weeks to ≤1 year	3
>1 year	2

C.2.3.4.2 Probability of occurrence of a hazardous event (Pr)

The probability of occurrence of harm should be estimated independently of other related parameters Fr and Av. A worst-case assumption should be used for each parameter to ensure that SRCF(s) are not incorrectly assigned a lower SIL than is necessary. To prevent this from occurring, the use of a form of

task-based analysis is strongly recommended to ensure that proper consideration is given to estimation of the probability of occurrence of harm. This parameter can be estimated by taking into account the following.

a) Predictability of the behaviour of component parts of the machine relevant to the hazard in different modes of use (e.g. normal operation, maintenance, fault finding).

   This will necessitate careful consideration of the control system especially with regard to the risk of unexpected start up. Do not take into account the protective effect of any SCS. This is necessary in order to estimate the amount of risk that will be exposed if the SCS fails. In general terms, it shall be considered whether the machine or material being processed has the propensity to act in an unexpected manner.

   The machine behaviour will vary from very predictable to not predictable but unexpected events cannot be discounted.

   NOTE Predictability is often linked to the complexity of the machine function.

b) The specified or foreseeable characteristics of human behaviour with regard to interaction with the component parts of the machine relevant to the hazard. This can be characterised by:

   — stress (e.g. due to time constraints, work task, perceived damage limitation), and/or

   — lack of awareness of information relevant to the hazard. This will be influenced by factors such as skills, training, experience, and complexity of machine/process.

   These attributes are not usually directly under the influence of the SCS designer, but a task analysis will reveal activities where total awareness of all issues, including unexpected outcomes, cannot be reasonably assumed.

   "Very high" probability of occurrence of a hazardous event should be selected to reflect normal production constraints and worst-case considerations. Positive reasons (e.g. well-defined application and knowledge of high level of user competences) are required for any lower values to be used.

   Any required or assumed skills, knowledge, etc. should be stated in the information for use.

Select the appropriate row for probability of occurrence of hazardous event (Pr) of Table C.5. Indicate the appropriate number under the Pr column in Table C.7.

Table C.5 — Probability (Pr) classification

Probability of occurrence	Probability (Pr)
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

C.2.3.4.3 Probability of avoiding or limiting harm (Av)

This parameter can be estimated by taking into account aspects of the machine design and its intended application that can help to avoid or limit the harm from a hazard. These aspects include, for example,

— sudden, fast, or slow speed of appearance of the hazardous event;

— spatial possibility to withdraw from the hazard;

— the nature of the component or system, for example, a knife is usually sharp, a pipe in a dairy environment is usually hot, electricity is usually dangerous by its nature but is not visible; and

— possibility of recognition of a hazard, for example, electrical hazard: a copper bar does not change its aspect whether it is under voltage or not; to recognize if one needs an instrument to establish whether electrical equipment is energised or not; ambient conditions, for example, high noise levels can prevent a person hearing a machine start.

Select the appropriate row for probability of avoidance or limiting harm (Av) of Table C.6. Insert the appropriate number under the Av column in Table C.7.

Table C.6 — Probability of avoiding or limiting harm (Av) classification

Probability of avoiding or limiting harm (Av)	Probability (Pr)
Impossible	5
Rarely	3
Probable	1

C.2.3.5 Class of probability of harm (Cl)

For each hazard and, as applicable, for each severity level, add up the points from the Fr, Pr, and Av columns and enter the sum into the column Cl in Table C.7.

Table C.7 — Parameters used to determine class of probability of harm (Cl)

Serial no.	Hazard	Se	Fr	Pr	Av	Cl
1						
2						
3						
4						

C.2.3.6 SIL assignment

Using Table C.8, where the severity (Se) row crosses the relevant column (Cl), the intersection point indicates whether action is required. The boxes indicate the SIL x assigned as the target for the SRCF. The boxes indicate (OM) should be used as a recommendation that other measures (OM) be used.

Table C.8 — SIL assignment matrix

Severity (Se)	Class (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

EXAMPLE For a specific hazard with an Se assigned as 3, an Fr as 4, an Pr as 5, and an Av as 5, then:

Cl = Fr + Pr + Av = 4 + 5 + 5 = 14

Using Table C.8, this would lead to a SIL 3 being assigned to the SRCF that is intended to mitigate against the specific hazard.

C.2.4 User's guide for risk graph in accordance with IEC 61511-3:2016 (i.e. Table C.2)

C.2.4.1 Hazard identification/indication

Indicate the hazardous event, including those from reasonable foreseeable misuse, whose risks are to be reduced by implementing a safety instrumented function (SIF). List them in the hazardous event and safety instrumented function column in Table C.2.

C.2.4.2 Risk estimation

The risk graph matrix in accordance with IEC 61511-3:2016 is used for SIL assignment of safety instrumented functions. Integrity levels are established by combining the risk graph consequence parameter C and the likelihood summarized as the risk graph parameters F, P, and W. Individual integrity levels for health (H), environmental (E), and financial (F) hazards could be determined. The overall target SIL of the considered safety instrumented function is the maximum determined integrity level.

Parameters are shown in Figure C.2 and should be derived from the following:

— consequence of harm (C), and

— probability of occurrence of that harm, which is a function of:

  — occupancy parameter (F) which is the probability that the exposed area is occupied at the time of the hazardous event;

  — avoidance parameter (P) which is the probability that exposed persons are able to avoid the hazardous situation, which exists if the SIF fails on demand;

  — demand rate parameter (W) which is the residual demand rate or frequency of the hazardous event if considering SIF is not implemented.

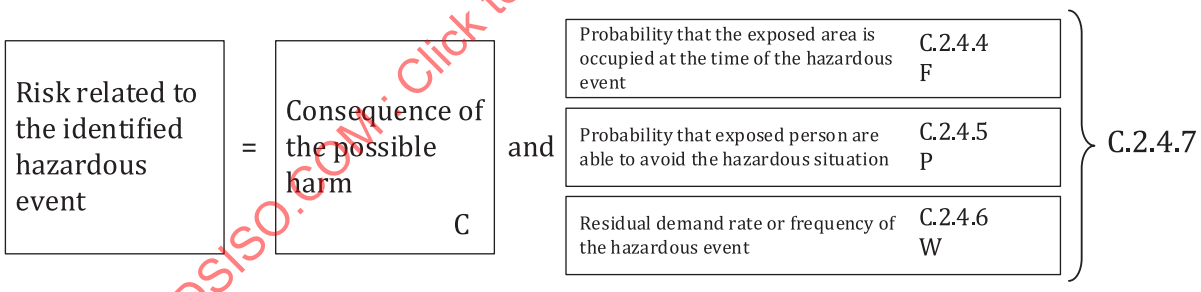


Figure C.2 — Parameters used in risk estimation by IEC 61511-3:2016

C.2.4.3 Consequence parameter selection

Consequence parameter represents number of fatalities and/or serious injuries likely to result from the occurrence of the hazardous event. It is determined by calculating the numbers in the exposed area when the area is occupied, taking into account the vulnerability to the hazardous event.

Severity level (C) is the estimated consequence of the hazardous event. Select proper level for health (H), environmental (E), and financial (F) hazards. Fill in the chosen severity letter (A-F) for each individual hazard in the C column.

NOTE Determining proper severity levels presupposes consequence categories calibrated to meet the tolerable risk levels established by company risk management and authorities.

For details in severity level in consequence, see Table C.9, C.10, and C.11.

Table C.9 — Severity level in consequence – Health hazard (*H*)

C	Health hazard (*H*)	Probability loss of life	Max. health consequences due to the hazardous event	Additional comments to the health consequence categories
C_F	Catastrophic	PLL > 1	Several (three or more) dead Many (10 or more) critical injured	Several fatalities likely
C_E	Extensive	PLL = 0,1 – 1,0	Some (one to two) dead Several (three or more) critical injured	Individual fatality/fatalities likely
C_D	Serious	PLL = 0,01 – 0,1	Some (one to two) critical injuries Several (3 or more) injured	Several lost time injury/injuries, one or some lasting disablement Fatality/fatalities not likely but possible
C_C	Considerable	PLL < 0,01	Some (one to two) injuries Serious discomfort	One or some lost time injury/injuries Minor probability of lasting disablement, fatality improbable
C_B	Marginal	PLL = 0	Minor injury/injuries Lasting discomfort	No lost time injury/injuries, medical treatment required
C_A	Negligible	PLL = 0	Negligible injury/injuries Temporary discomfort	No lost time injury/injuries, no medical treatment required
NOTE C: Severity level.				

Table C.10 — Severity level in consequence – Environmental hazard (*E*)

C	Environmental hazard (*E*)	Effluent Influence	Effluent Extension	Max. environmental consequences due to the hazardous event	Additional comments to the environmental consequence categories
C_F	Catastrophic	Lasting	Wide	Wide permanent or long-time harm Decontamination impossible or hard	A liquid spill into river or sea; a wide vapour or aerosol release The effluent causes lasting or permanent damage to plants and wildlife.
C_E	Extensive	Lasting	Confined	Confined permanent or long-time harm Decontamination impossible or hard	A liquid spill to ground water; a confined vapour or aerosol release The effluent causes lasting or permanent damage to plants and wildlife.
C_D	Serious	Lasting	Limited	Limited permanent or long-time harm Decontamination impossible or hard	Onsite liquid spill; a limited vapour or aerosol release (within fence) The effluent causes lasting or permanent damage to plants and wildlife.
C_C	Considerable	Temporary	Wide/ Confined	Wide to confined temporary harm Decontamination easy or not needed	A liquid spill into river or sea; a limited vapour or aerosol release The effluent causes temporary damage to plants and wildlife.
C_B	Marginal	Temporary	Limited	Limited (on site) temporary harm Decontamination easy or not needed	Onsite liquid spill, a limited vapour or aerosol release (within fence) The effluent causes temporary damage to plants and wildlife.
C_A	Negligible	Negligible		Negligible environmental harm Decontamination not needed	Moderate leak from flange or valve Small liquid spill or small soil pollution not affecting ground water. Negligible environmental effects.
NOTE C: Severity level.					

Table C.11 — Severity level in consequence — Financial hazard (*F*)

C	Financial harm (F)	Damaged property (k€)	Production loss (k€)	Max. financial consequences due to the hazardous event	Additional comments to the financial consequence categories
C_F	Catastrophic	>10 000	>50 000	Devastating loss off production, market share and image	Devastating damage to production unit and/or plant Event causing or requiring a production stop for more than a year
C_E	Extensive	1 000 – 10 000	5 000 - 50 000	Extensive loss of production Large loss of market share and/or image	Extensive damage to equipment and/or property Event causing or requiring a lasting production stop of several months
C_D	Serious	100 – 1 000	500 - 5 000	Large loss of production Considerable loss of market share and/or image	Serious damage to equipment and/or property Event causing or requiring a lasting production stop up to a month
C_C	Considerable	10 - 100	50 -500	Considerable loss of production. Marginal loss of market share	Considerable damage to equipment and/or property Event causing or requiring a lasting production stop up to a week
C_B	Marginal	1-10	5-50	Minor loss of production No loss of market share and/or image	Minor damage to equipment Event causing or requiring a day of production stop
C_A	Negligible	<1	<5	Negligible loss of production No loss of market share and/or image	Negligible damage to equipment Event causing or requiring a temporary (hours) production stop
NOTE C: Severity level.					

C.2.4.4 Occupancy parameter selection

Occupancy parameter represents the probability that the exposed area is occupied at the time of the hazardous event, determined by calculating the fraction of time the area is occupied at the time of the hazardous event. This should take into account the possibility of an increased likelihood of persons being in the exposed area in order to investigate abnormal situations which can exist during the build-up to the hazardous event (consider also if this changes the C parameter).

Exposure rate (F) is the probability that the exposed area is occupied at the time of the hazardous event. The exposure rate is only valid for health (H) risks. If occupancy is permanent or if credit already has been given for a reduced occupancy likelihood when the health severity level was chosen, the "Permanent" alternative (FD) shall be chosen. Exposure rate FC shall be chosen if occupancy is frequent or if the occupancy is dependent on the hazardous situation. Exposure rate FB should be chosen if the area is occupied just occasionally and human presence is obviously independent of the hazardous situation. Exposure rate FA should only be chosen if the hazardous area is confined and human presence rare and independent of the hazardous situation. Fill in the selected correlating number (0-2) in the P column. 1 is predefined for the environmental (E) and financial (F) hazards.

C.2.4.5 Avoidance parameter selection

Avoidance parameter represents probability that exposed persons are able to avoid the hazardous situation, which exists if the safety instrumented function fails on demand. This depends on there being independent methods of alerting the exposed persons to the hazard prior to the hazard occurring and there being methods of escape.

Avoidance probability (P) is the probability of avoiding the hazardous event even if the considered safety function fails to prevent the event. Normal choice is PB "Avoidance conditions not fulfilled". PA could be chosen individually for the health hazard (H) if all persons in the hazardous area are likely

evacuated to a safe area in time if the SIF fails on demand. Besides time are independent facilities for alerting and evacuating all people in the hazardous area required. PA could also be claimed if the hazardous event is likely avoided in time by manual operator actions. In this case, PA is also relevant for the environmental (E) and financial (F) hazards. Independent facilities for alerting the operator of the functional failure and for manually bringing the process to a safe state are an absolute demand. The access of time is also a very important requirement for claiming PA, and 1 h is a minimum requirement between operator alert and the hazardous event for taking credit for "Possibility of avoidance" (PA). Fill in the correlating number (0 or 1) of the selected avoidance parameter in the P column.

C.2.4.6 Demand rate parameter selection

Demand rate parameter represents the number of times per year that the hazardous event would occur in the absence of the safety instrumented function under consideration. This can be determined by considering all failures, which can lead to the hazardous event and estimating the overall rate of occurrence. Other protection layers should be included in the consideration.

The demand rate parameter (W) is selected by estimating or calculating the residual demand rate or frequency of the hazardous event if the considered SIF not is implemented. This frequency can be determined by combining frequencies of failures and other initializing events leading to the hazardous event. Credit should be given for non-SIS-implemented safety barriers. The layer of protection analysis (LOPA) is a recommended frequency analysis method. The total risk reduction credit for barriers implemented in the normal control system (BPCS), including alarms and operator response, is maximized to 10 times by definition in the IEC 61511:2016 series (risk reduction factor >0,1). Fill in the chosen number correlating to the estimated or calculated residual demand rate in column W.

C.2.4.7 Risk graph matrix SIL-assignment

Finally, add the F, P, and W numbers for each of the health (H), environmental (E), and financial (F) hazards. Fill in the resulting parameter sum in the "Likelihood" column of the form. Use the risk graph matrix to read out the safety integrity level (SIL) for each and one of the hazards by combining its severity letter (A-F) with its likelihood sum (1-12). The overall target SIL equals the maximum determined SIL.

Annex D
(informative)

Example of a risk assessment for one safety instrumented function using the method according to the IEC 61511:2016 series

D.1 General

This annex provides a partial example of the procedures that are used when designing a system in accordance with the IEC 61511:2016 series for a protective system using method D. This example is illustrative only, is not exhaustive, and should not be used for an actual system.

D.2 Concept description of equipment under control

A heat-treating furnace operates at 500 °C with a negative pressure, non-flammable atmosphere. It has 40 burners with half on each length of the furnace. There are two combustion air blowers, one on each side, each serving half the burners. There are two fuel flow control valves on the main header, each serving one side with half the burners. The blower air and the fuel flows are modulated in order to maintain the process temperature. The fuel and air flow control loops are provided through a central control system. There is a minimum airflow of 25 % and a minimum fuel flow of 10 %. The fuel flow is also limited to a maximum of 80 % of control valve setting which is 100 % of normal firing rate. The fuel pressure to the burners is modulated from 0,25 kPa [gauge] to 14 kPa [gauge] and the air pressure is modulated from 2,5 kPa [gauge] to 15 kPa [gauge].

The furnace is located in a large metal fabrication facility (10 000 m^2) with 200 workers. There are welding, cutting, grinding, and other spark-producing operations around the furnace.

The furnace is 20 m long by 2 m wide. It has six stacks that are tied to a common manifold, which is connected to an exhaust stack. The furnace operates continuously. The charge enters and leaves the furnace through doors located on either end. The process is batch operated where each batch takes from 2 h to 12 h. The furnace walls are designed for an overpressure condition of 70 kPa [gauge]. There is no explosion relief door.

The blower is belt driven with external bearings. Its motor is started and controlled by a variable speed drive that is driven from the central control through a (4 to 20) mA signal. Each burner has a damper that is used for local trimming of the combustion air to that burner and can be closed while a burner is offline for maintenance.

The control valve is a motor operated butterfly valve with a line voltage powered actuator. The control signal is (4 to 20) mA provided from the central control system.

D.3 Hazard and risk assessment

A loss of combustion air will result in an accumulation of unburned fuel in the firebox. Subsequent re-establishment of the combustion air source could lead to a deflagration and possible explosion.

D.3.1 Initiating events

Blower system failure:

a) bearing (inboard bearing, outboard bearings, unbalanced wheel);

b) motor failure (bearings, winding shorts, overload, breaker tripped);

c) VSD failure (short circuit, open circuit);

d) belt failure (wear and tear);

e) air inlet blocked (dirt, plate, cardboard, tarpaulins);

f) human error (blower shut off, block inlet);

g) human error (closed at wrong time or close wrong damper);

h) damper fastening screw wears loose due to vibration and damper closes.

Burner duct air leakage:

i) flexible duct leaks or breaks.

D.3.2 Hazard — Process deviation – insufficient combustion air

a) Insufficient air to one or more burners;

b) CO and unburned hydrocarbon build up in furnace;

c) unstable combustion.

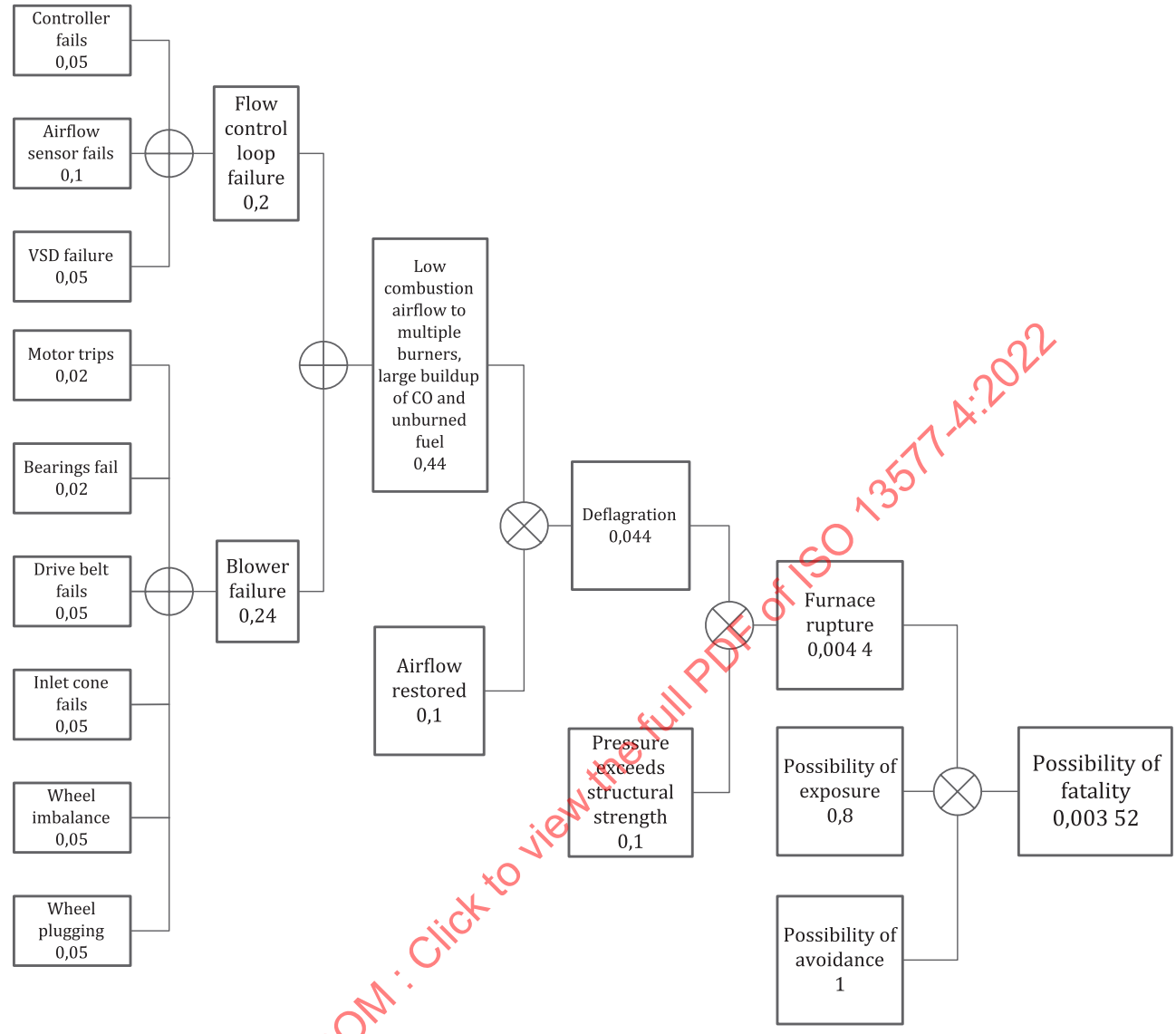
D.4 Consequences

a) Afterburning in the stack (negative pressure draws in air);

b) re-establishment of combustion air could lead to deflagration and possible explosion.

D.5 Event tree example

See Figure D.1.



Key

summation of event probability by a logical 'OR'

multiplication of event probability by a logical 'AND'

Figure D.1 — Event tree example

D.6 Protective system safety requirement specification

NOTE This clause contains examples of the possible content of the safety requirements specification, which need to be sufficient to design the protective system SIS and the application program.

D.6.1 General requirements

a) If at any point during the furnace operating sequence the combustion air flow to the burners fall below 20 % of the maximum airflow, the fuel supply to all related burners shall be shut off within the process safety time.

b) The motor run status from the VSD shall be wired directly to the logic solver to provide further pre-emptive trip functionality. The blower running status shall provide a risk reduction of at least 10.

c) The combustion air flow sensors shall be incorporated in the start-up sequence to ensure the airflow is sufficient to properly purge the furnace.

d) After each safety shutdown, the combustion chamber shall be purged a minimum of five volume changes. During the purge, the airflow as measured by the sensor shall measure greater than 50 % of the maximum airflow rate. If the airflow falls below this flow rate, the purge shall not continue.

e) The safety instrumented function shall meet a risk reduction factor (RRF) of 352 (SIL 2) with a testing interval of 2 years in order to coincide with the plant turnaround.

NOTE Without additional measures, the risk of fatality is 0,003 52 (see Figure D.1). When acceptable risk is 10-5, then the protective system SIS provides a risk reduction of (10-5 / 0,003 52) = 0,002 84, which is RRF = 352 (SIL 2).

f) The safe state for the system is to have fuel isolated from the furnace. The fuel automatic shut-off valves shall be fail closed.

g) The safe state for the combustion air blower shall ensure a minimum airflow through the furnace.

h) During a manual emergency shutdown, the safe state is to fully isolate all fuel and ignition sources. Loss of power shall result in the same fail position as manual emergency shutdown.

i) Loss of actuating media (e.g. pneumatic, hydraulic) shall result in fuel automatic shut-off valves failing closed.

j) The demand rate is less than once per year, i.e. low demand mode of operation. The sources of demand are due to equipment hardware failure, control loop failure, and human error. It is assumed that the operators are trained with a documented formal training process.

k) The spurious trip rate shall not exceed once in 10 years for each safety function.

l) The safety function shall be proof tested with 90 % coverage each 2 years. In order to ensure 90 % coverage, the airflow shall be reduced below the trip point to verify that the output to the automatic shut-off valves is de-energized. During this test, the fuel shall be manually isolated from the furnace such that the safety of the furnace is not compromised. De-energizing of the automatic shut-off valves shall be tested separately using some other method, such as manually closing the upstream fuel valve and checking for automatic shutdown of the automatic shut-off valves upon loss of flame from the flame scanner. Once the automatic shut-off valves are closed, they shall be leak tested.

m) The process safety time for complete isolation of the fuel to the side of the furnace where air flow is below the trip points shall be less than 10 s. This process safety time is based on LFL calculations (not shown in this example) that an accumulation of unburned fuel within 10 s will not result in an explosive mixture of sufficient energy to exceed the strength of the TPE.

n) The system response time from the time the airflow drops below the trip point to the time the fuel is completely isolated to the associated side of the furnace shall be within 5 s. This is half the process safety time.

D.6.2 Safety sensor functional requirements

— Each side of the furnace shall have two safety flow transmitters voted as 1oo2D[4)] providing a hardware fault tolerance of 1.

4) 1oo2D: 1 out of 2 channel architecture with Diagnostics. 1oo2D is architecture with diagnostics, where either of the two channels can perform the safety function. For details, see IEC 61508-6:2010, Annex B.

— The airflow shall be measured directly using mass, velocity, or differential pressure methods. Downstream blockages shall not result in a false airflow reading such as would occur if static pressure is used to infer flow.

— A common flow element can be used for the basic process combustion control flow sensor, as well as the safety flow transmitters; however, all sensing lines, root valves, and connection points shall be separate to prevent common cause failures.

— All aspects of the safety manual shall be reviewed for the safety sensor.

— The airflow sensor shall:

  a) be a different model from the process combustion control airflow sensor but it can be from the same manufacturer (this is to minimize common cause factors),

  b) be suitable for use between temperatures of -20 °C to 60 °C,

  c) be compensated by a suitable downstream temperature element,

  d) be suitable for a high-vibration, heavy industrial environment (the sensor shall be securely mounted with adequate mechanical protection from shock and impact loads),

  e) be suitable for heavy industrial EMC environment,

  f) be suitable for a hazardous environment class I zone 1A T1,

  g) be provided with an IP 65 or better enclosure,

  h) be smart and with a diagnostics coverage factor of more than 80 % (the sensor shall revert to a low analogue output signal of less than 3,8 mA when a fault condition is detected),

  i) be configurable with a smart field programmer (such as a HART communicator); however, the communications shall be able to be switched off once the safety function is on line,

  j) be provided with an accuracy of at least 2 % for a period of more than 2 years without recalibration,

  k) be factory calibrated with a traceable calibration certificate,

  l) have a systematic capability of SC 3,

  m) be provided with a suitable SIL certificate, and

  n) be wired using 1,5 mm^2 twisted, shielded pair armoured instrument cable with the drain bonded at the logic solver side [the cable shall be run in a cable tray that is a minimum of 1 m from all high-voltage and large EMI-generating devices (motors, VSDs)].

— The sensing lines to the sensor shall:

  i) continuously rise with no low points or sags (the sensing lines shall be self-draining to the combustion air flow duct),

  ii) consider a minimum of 12 mm to prevent blockage and to ensure a fast response.

— The sensing line to the sensor shall be corrosion resistant 316 SST.

— The sensing line to the sensor shall be leak tested at a minimum of 10 kPa [gauge] with zero leakage over 30 min and where threaded, have no thread lubricant on the first two threads to avoid sensor plugging.

— Provisions shall be provided on each sensor for zeroing and testing. A suitable device is a three- or five-valve manifold with removable handles and suitable process connections for connecting a differential pressure calibrator.

— During safety operation, the sensor valve manifold shall have the handles removed.

— During testing, the handles are installed. A pressure calibrator shall be connected to the sensor and a differential pressure corresponding to 25 % and then 20 % shall be applied to one sensor. This shall cause the system to request a trip. Both sensors shall be tested during the proof test interval.

D.6.3 Logic solver requirements including alarming, external comparisons and HMI

— Each flow sensor with the 1oo2D pair shall be wired to separate 4 mA to 20 mA 12 bit isolated loop powered analogue input cards on the PLC.

— The process control sensor shall be wired to the central control system.

— The automatic shut-off valves for each burner shall be wired to separate 24 VDC digital output cards on the PLC.

— The safety logic solver shall provide a first order software filter of no more than 1 s.

— Where the self-diagnostics of a sensor detects a fault and provides an out-of-range signal to the logic solver, the logic solver shall vote out and the faulty sensor and the trip function shall revert to 1oo1. Under these conditions, an alarm shall be generated in the logic solver to indicate a faulty flow sensor. This alarm shall be re-alarmed every 4 h.

— The mean time to restoration (MTTR) for the 1oo2D function is assumed to be 72 h, if the risk assessment allows it.

— It is assumed that at least one spare airflow sensor is in stock at all times.

— The analogue value from each airflow sensor shall be communicated to the central control system. The value of the combustion process control flow signal shall be displayed along with deviation and fault alarms from the safety sensors. The HMI shall provide the option to display the analogue value of each airflow sensor from the safety system, but this can be switched off by the operator to only display the process control airflow sensor value.

— The update time of the HMI shall be less than 1 s.

— Alarms shall be audible and visual and recorded in a history log.

— Alarms shall be provided when either safety airflow sensor or the combustion process control airflow sensor falls below 25 % of maximum airflow to warn the operator of an impending trip.

— A deviation alarm shall be generated when either of the 1oo2D airflow safety sensors measures a deviation of more than 10 % from combustion process control airflow sensor. 10 % is based on system operation with an O_2 level of 3 % in the exhaust gas, which corresponds to operating the burner at approximately 15 % excess air level.

— The status of each valve shall be displayed on the HMI. A valve position switch mismatch shall generate an alarm.

— Where the combustion air flow is the cause of a fuel trip, it shall be displayed on the HMI as a first out.

— For detailed requirements, see the logic solver specifications document.

D.6.4 Final element requirements

— Each burner shall have two de-energize to trip electric (24 VDC) actuator automatic shut-off valves piped in series.

— The automatic shut-off valves shall have closed position switch feedback that is wired to the logic solver.

— The fuel shall be clean natural gas of constant calorific value. The fuel supply to the safety valves shall be filtered upstream in order to ensure particles no more than 100 microns are allowed to pass through. All piping downstream of the filter shall be thoroughly brush pigged (cleaned) prior to commissioning of the fuel system.

— Provisions shall be made available to test each automatic shut-off valve by placing pressure upstream of the valve and measuring pressure downstream of the valve.

— The automatic shut-off valves shall be:

  a) fire safe,

  b) tightly shut off and shall meet the requirements of the applicable standard for burner safety shut-off valves (as specified in ISO 23551-1),

  c) provided with upstream and downstream isolation valves to allow online maintenance and testing,

  d) suitable for natural gas at temperatures from -20 °C to 60 °C,

  e) suitable for ambient temperatures from -20 °C to 60 °C,

  f) suitable for a hazardous environment class I zone IIb TC3,

  g) suitable for pressures up to 10 bar g,

  h) suitable for a high-vibration, high-EMC heavy industrial environment,

  i) flanged to ensure ease or removal and replacement, and

  j) externally corrosion-resistant or painted.

— During testing, the automatic shut-off valves shall have a leakage rate of not more than 50 dm^3/h (based on ISO 23551-4).

— A burner can be isolated for maintenance if the automatic shut-off valve fails the leak test. The furnace can operate with one burner out of service.

— At least one automatic shut-off valve is to be kept in stock as a spare part.

D.6.5 Manual intervention requirements

— The low airflow safety function or loss of airflow safety function shall be manually reset to prevent automatic restarting of the equipment. The manual reset button shall be located near to the equipment and require the operator to physically inspect the equipment prior to re-energizing.

— A separate and independent manual trip function shall be provided to de-energize all fuel and combustion air directly. Three manual trip buttons shall be provided: one in the control room, one near to the furnace, and one a minimum of 20 m away. The manual trip function shall be in accordance with ISO 13850 mushroom head push to trip button with a guard to prevent spurious trips. The manual trip shall be tested along with the other devices in the safety function every 2 years.

D.6.6 Start-up requirements

The combustion air blower is in operation when the ESD button is not de-energized and the blower disconnect is set to On. There should therefore be combustion air flow at all times and there is no requirement to bypass the combustion air flow during start-up.

During the purge, the combustion air flow is required to be greater than 60 % of maximum airflow in order to ensure a thorough purge. This shall be an additional permissive for the duration of the purge. If the airflow falls below the minimum purge rate, the purge shall be stopped and require a restart.

During the purge, the PLC shall measure the combustion air flow and measure the required purge time in order to ensure at least five volume changes through the furnace and associated flue passages.

Annex E
(informative)

Examples for protective functions

E.1 General

For a better and easier understanding of the three methods (A, BC, and D), this annex shows some practical examples on how to build the hardware configurations in each method and provides the main conditions for a clear comparison.

Examples for wiring are given in Annex B.

Only a few commonly used configurations are shown in these examples. Other options are possible since not everything is listed here in detail.

The principles of the three methods (A, BC, or D) are used as follows:

— Method A, 4.2.2: wired system, all devices comply with relevant product standards (see Figure 4); SIL- / PL-calculation is not required;

— Method BC, 4.2.3: combination of devices meeting relevant product standards with devices for which no relevant product standard exits (see Figure 5). SIL- / PL-calculation for the subsystems with no product standard is needed;

— Method D, 4.2.4: full requirement in accordance with the IEC 61508:2010 series, the IEC 61511:2016 series, IEC 62061:2021, or ISO 13849-1:— (see Figure 6), and SIL- / PL-calculation is mandatory for each safety function.

An overview of the different requirements and combinations (input, logic, and output) is given in Table E.1.

E.2 and E.3 show examples of safety functions and subfunctions.

Safety functions with minimum SIL 3 or PL e should have at least an 1oo2D architecture, or HFT = 1.

With methods BC and D, diagnostics of the closure of the valves should be implemented where possible. Options of diagnostics for the closure of the safety relevant shut-off function are:

— a valve proofing system: valve proofing done before start of the relevant burners(s) of the TPE, or just after the valves close in case of no heat demand; or

— each valve equipped with a closed position indicator switch, interlocked in the safety chain; or

— the use of flame monitoring (see NOTE 2 in this subclause).

NOTE 1 Diagnostics in high cycle applications as identified in ISO 13577-2 is not normally feasible with the above approach.

NOTE 2 In case burners and respectively safety shut-off valves operate in high demand mode, every time the burner is switched off by the logic solver, it

a) can de-energize valve 1 of the two valves;

b) detects valve 1 has closed (for example by detecting no flame within a predefined time period as diagnostic);

c) closes valve 2 of the two valves; and

d) starts this procedure with valve 2 the next time it switches off the burner.

Options of diagnostic for the safety relevant functions are:

— cross monitoring of input signals and comparing results within the logic solver;

— temporal and logical software monitor of the program flow; and

— detection of static faults.

It is possible to combine safety functions for high and low demand mode of operation.

Each safety function can be implemented following method A, BC, or D. Method A does not require reliability data, nor any calculation of reliability level. Component conformity to product standards ensure the safety level of the safety functions.

The risk assessment numbers in Table E.1 refer to Table C.1 and Table C.2.

Table E.1 — Overview of examples of different requirements for safety relevant systems

SRP/CF or SIF N°	Safety function	Level required	Method	Examples of safety functions	Examples of sub-systems	Demand mode	Standards	Reliability data
10	High temperature monitoring	**Not applicable**	**A**			Not applicable		Not required
		PL c SIL 1	**BC**		IS.1, IS.4	High or low demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required; or B_{10D}, $MTTF_D$, λ_D, PFH_D in high demand subsystems; or λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type in low demand subsystems
			D		IS.4	High demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508 series	B_{10D}, $MTTF_D$, λ_D, PFH_D
						Low demand	the IEC 61508:2010 series, the IEC 61511:2016 series	λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type, etc.
10	High temperature monitoring	**Not applicable**	**A**			Not applicable		Not required
		PL d SIL 2	**BC**	E.14, E.26	IS.2, IS.5	High or low demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required; or B_{10D}, $MTTF_D$, λ_D, PFH_D in high demand subsystems; or λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type in low demand subsystems
			D		IS.5	High demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series	B_{10D}, $MTTF_D$, λ_D, PFH_D
						Low demand	the IEC 61508:2010 series, the IEC 61511:2016 series	λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type, etc.
NOTE ISO 13577-2: —, Annex J provides a list of regional standards.								

Table E.1 *(continued)*

SRP/CF or SIF N°	Safety function	Level required	Method	Examples of safety functions	Examples of sub-systems	Demand mode	Standards	Reliability data
10	High temperature monitoring	**Not applicable**	**A**			Not applicable		Not required
		PL e SIL 3	**BC**	E.14, E.27	IS.3, IS.6	High or low demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required; or B_{10D}, $MTTF_D$, λ_D, PFH_D in high demand subsystems; or λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type in low demand subsystems
			D	E.27	IS.6	High demand	ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series	B_{10D}, $MTTF_D$, λ_D, PFH_D
						Low demand	the IEC 61508:2010 series, the IEC 61511:2016 series	λ_S, λ_{DU}, $\lambda_{DD,}$ SFF, arch type, etc.
12	High / low pressure monitoring	**Not applicable**	**A**	E.11	IS.10, IS.13	Not applicable	IEC 60730-2-6:2019	Not required
		PL c SIL 1	**BC**	E.12	IS.10, IS.13, IS.16	High or low demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required or PFH_D, respectively
			D		IS.16	High demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series	B_{10D}, $MTTF_D$, λ_D, PFH_D

NOTE ISO 13577-2: —, Annex J provides a list of regional standards.

Table E.1 *(continued)*

SRP/CF or SIF N°	Safety function	Level required	Method	Examples of safety functions	Examples of sub-systems	Demand mode	Standards	Reliability data
12	High / low pressure monitoring	**Not applicable**	**A**		IS.11, IS.14	Not applicable	IEC 60730-2-6:2019	Not required
		PL d SIL 2	**BC**	E.13, E.16, E.20, E.26, E.27	IS.11, IS.14, IS.17	High or low demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required or PFH_D, respectively
			D	E.16	IS.17	High demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series	B_{10D}, $MTTF_D$, λ_D, PFH_D
						Low demand	the IEC 61508:2010 series, the IEC 61511:2016 series	λ_S, λ_{DU}, λ_{DD}, SFF, arch type, etc.
12	High / low pressure monitoring	**Not applicable**	**A**		IS.12, IS.15	Not applicable	IEC 60730-2-6:2019	Not required
		PL e SIL 3	**BC**	E.17	IS.12, IS.15, IS.18	High or low demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series, the IEC 61511:2016 series	Not required or PFH_D, respectively
			D		IS18	High demand	IEC 60730-2-6:2019 or ISO 13849-1:—, IEC 62061:2021, the IEC 61508:2010 series	B_{10D}, $MTTF_D$, λ_D, PFH_D
						Low demand	the IEC 61508:2010 series, the IEC 61511:2016 series	λ_S, λ_{DU}, λ_{DD}, SFF, arch type, etc.
NOTE ISO 13577-2: —, Annex J provides a list of regional standards.								

Table E.1 *(continued)*

SRP/CF or SIF N°	Safety function	Level required	Method	Examples of safety functions	Examples of sub-systems	Demand mode	Standards	Reliability data
n.a	Flame monitoring	**Not applicable**	**A**	E.10, E.26, E.28	IS.40	Not applicable	IEC 60730-2-5:2013+AMD1:2017+ AMD2:2020 CSV	Not required
		PL e **SIL 3**	**B**, **C**	E.15, E.18, E.26, E.28	IS.41	High or low demand	IEC 61508:2010 series	Not required, or PFH_D or PFD, respectively
			D	E.15, E.18, E.27, E.28	IS.41	High demand	IEC 60730-2-5:2013+AMD1:2017+ AMD2:2020 CSV and the IEC 61508:2010 series	PFH_D
						Low demand	IEC 60730-2-5:2013+AMD1:2017+ AMD2:2020 CSV and the IEC 61508:2010 series	PFD

NOTE ISO 13577-2: —, Annex J provides a list of regional standards.

E.2 Examples of subfunctions

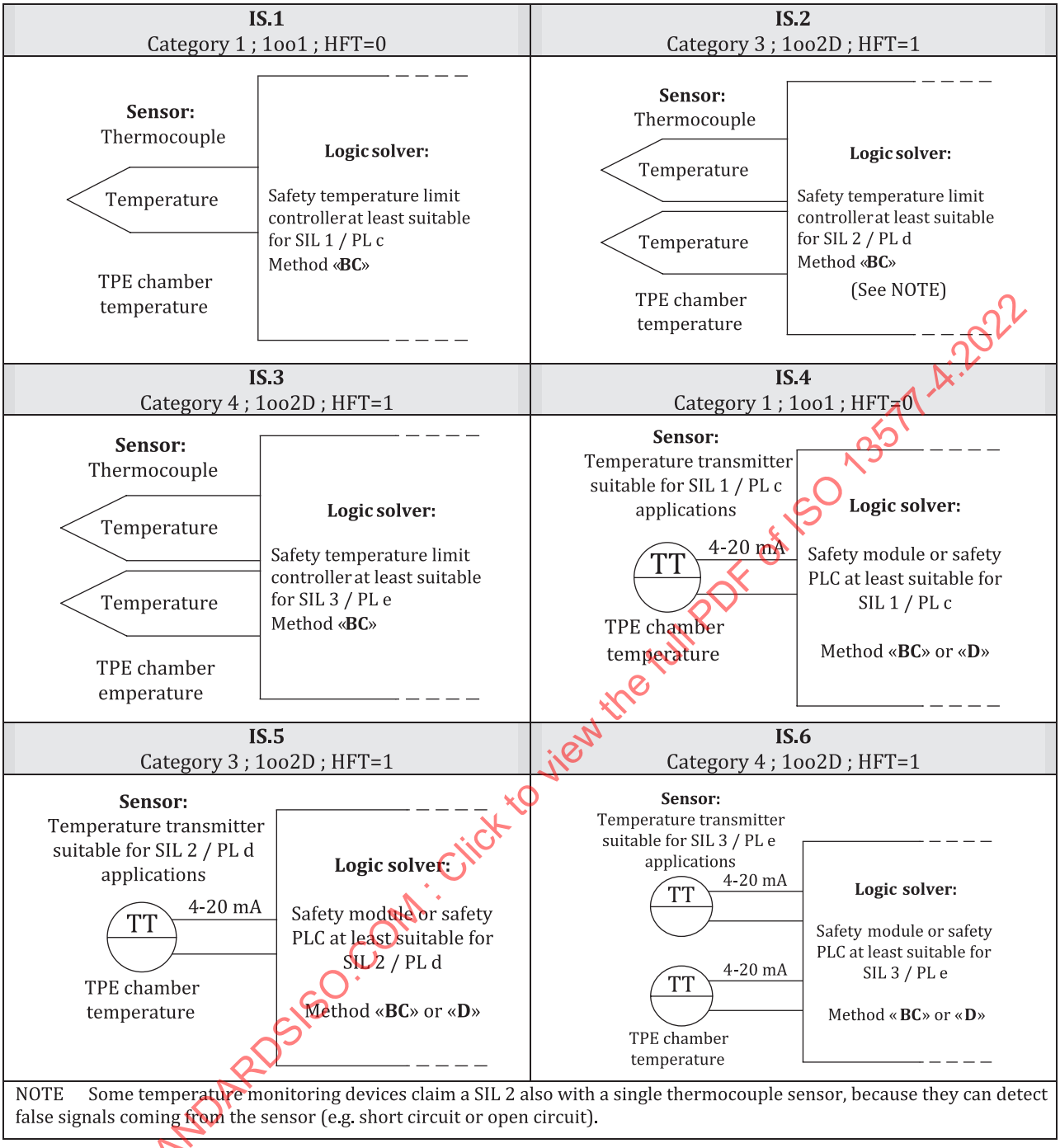
E.2.1 Overview of different requirements for input subfunctions

In high demand, “SIL n / PL n capable” or “certified suitable for SIL n or PL n applications” means that the component, based upon its reliability data and number of operations per year, reaches a PFH_D value such that the safety function can reach SIL n according to IEC 62061:2021, or PL n according to ISO 13849-1:—.

In low demand, “SIL n capable” means that both the component hardware and the software have systematic capability of “n”.

Safety relays, safety modules, or a safety PLC with certified hardware and software certified functional blocks, are used in method BC. A safety PLC with certified hardware and application software using other than certified functional blocks and complying with IEC 61508-3:2010, is used in method D. Safety relays are considered having digital input and digital output only.

See Figures E.1 to E.7 for examples of subfunctions.



NOTE Some temperature monitoring devices claim a SIL 2 also with a single thermocouple sensor, because they can detect false signals coming from the sensor (e.g. short circuit or open circuit).

Figure E.1 — Temperature measuring

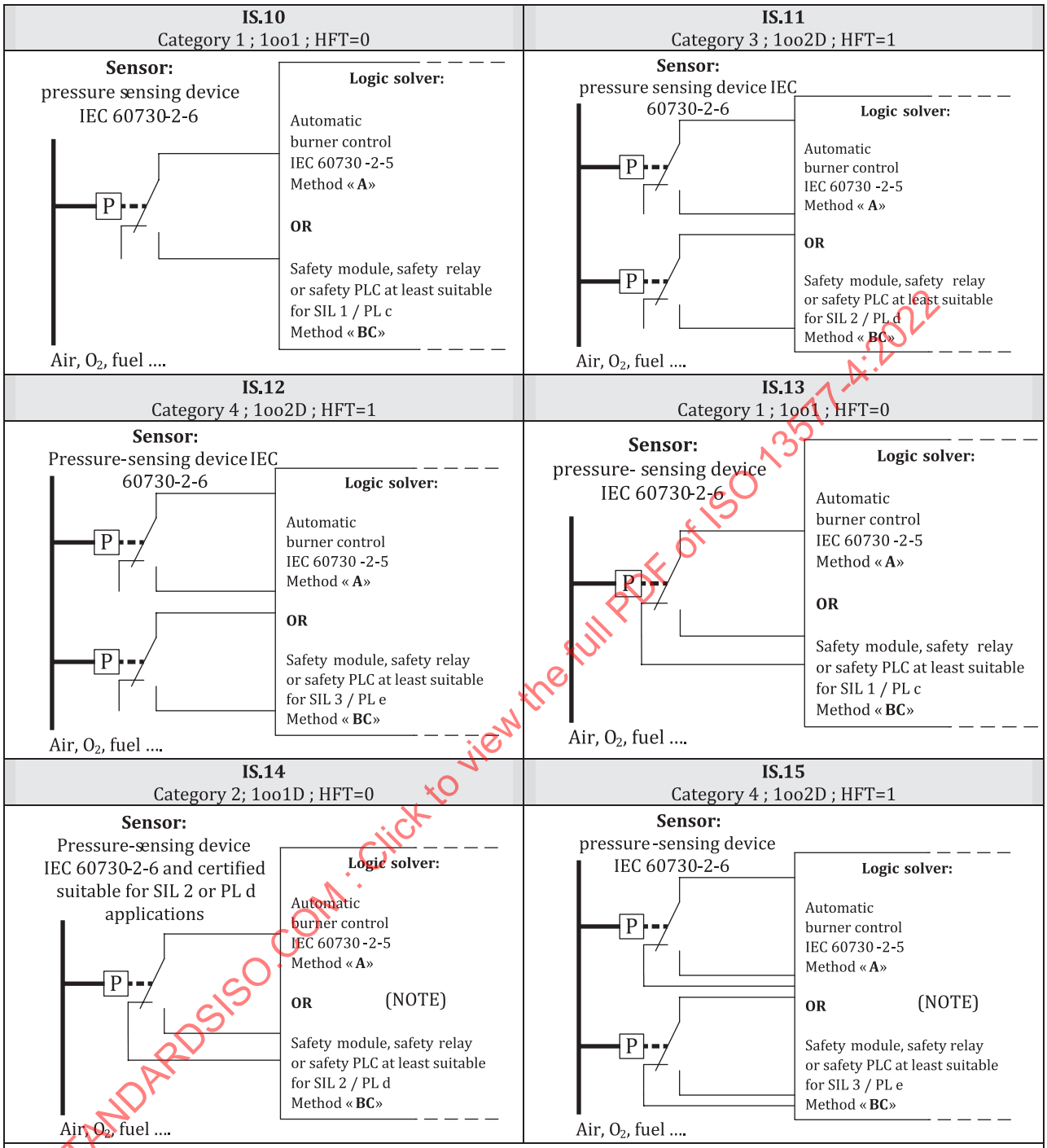


Figure E.2 — Pressure sensing and status detection

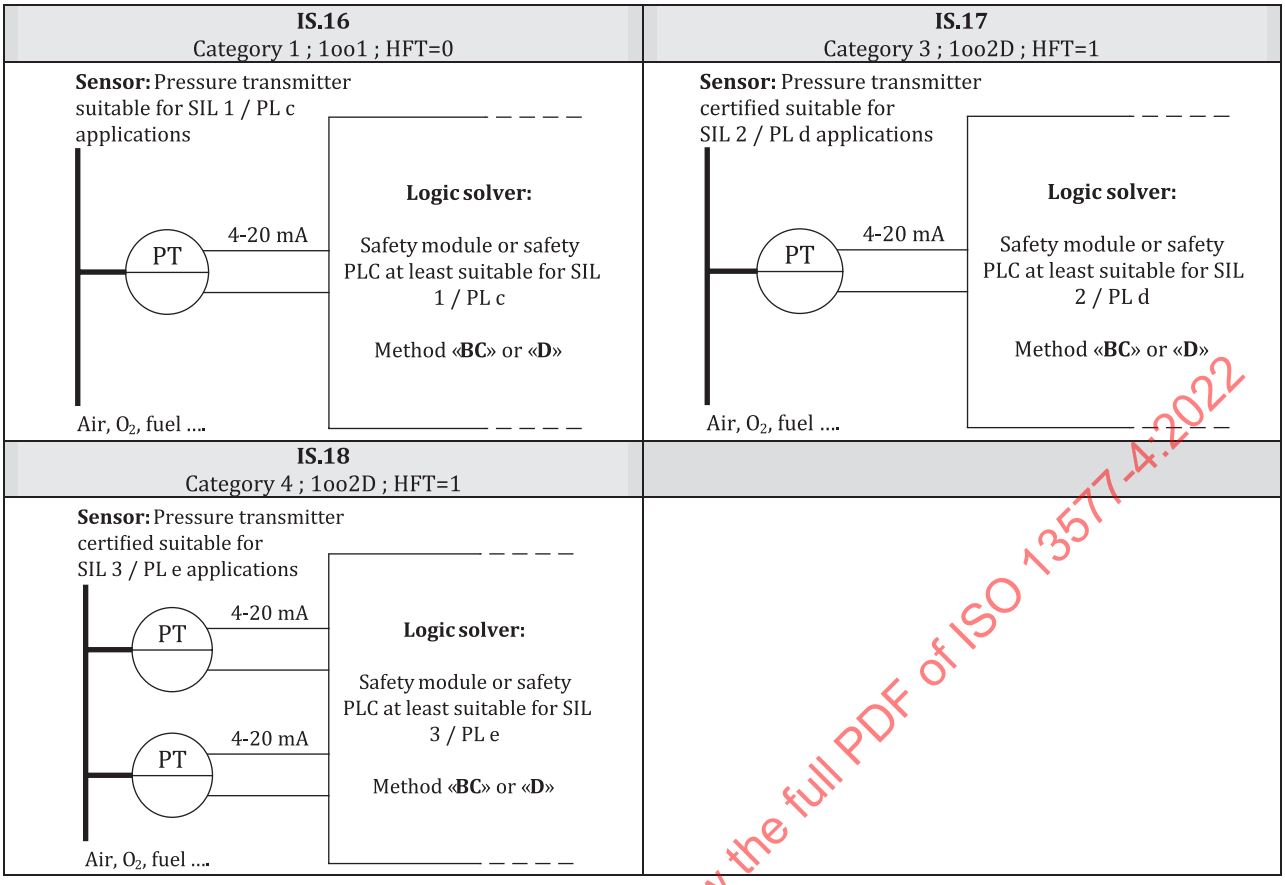


Figure E.3 — Pressure measuring

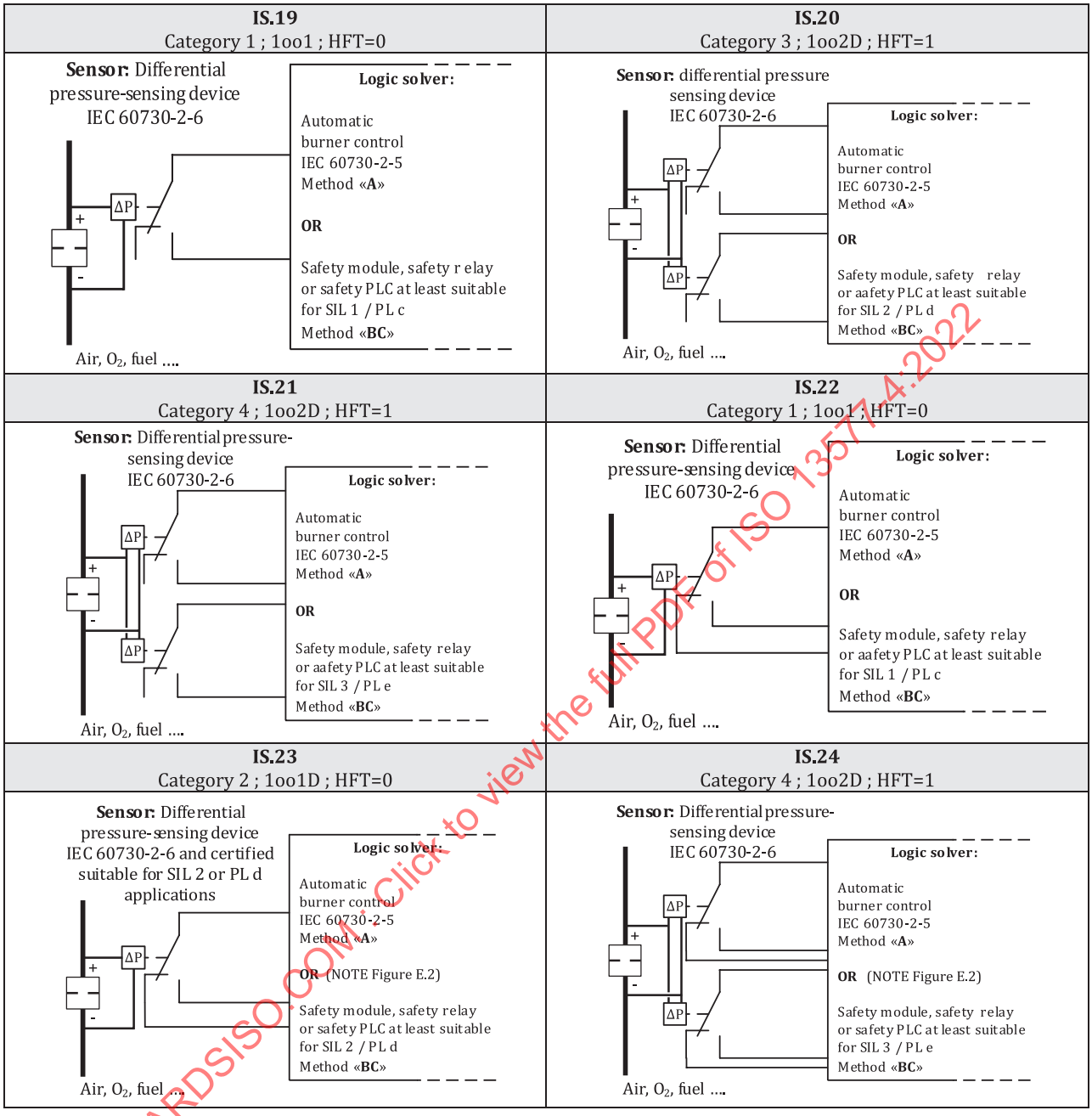


Figure E.4 — Flow sensing and status detection

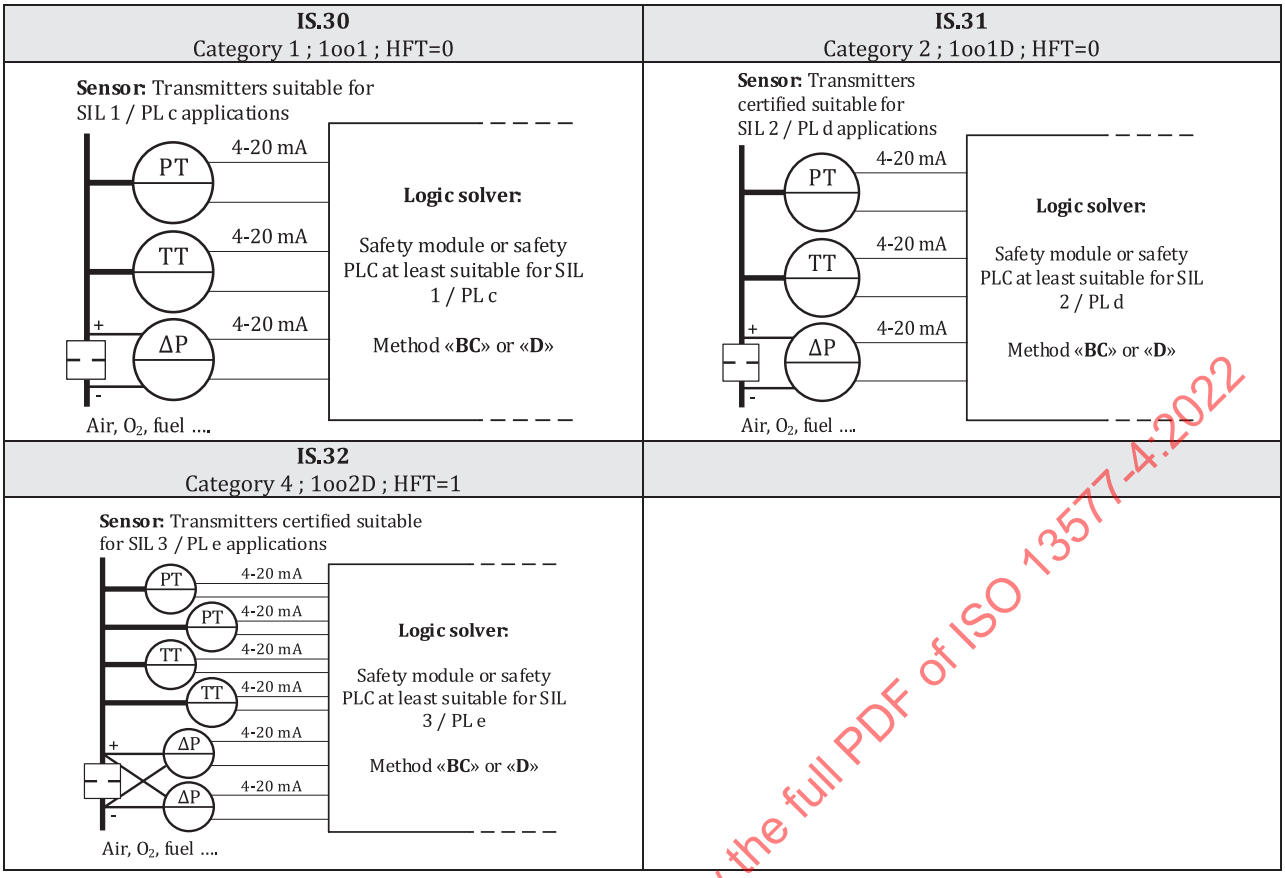


Figure E.5 — Mass flow measuring

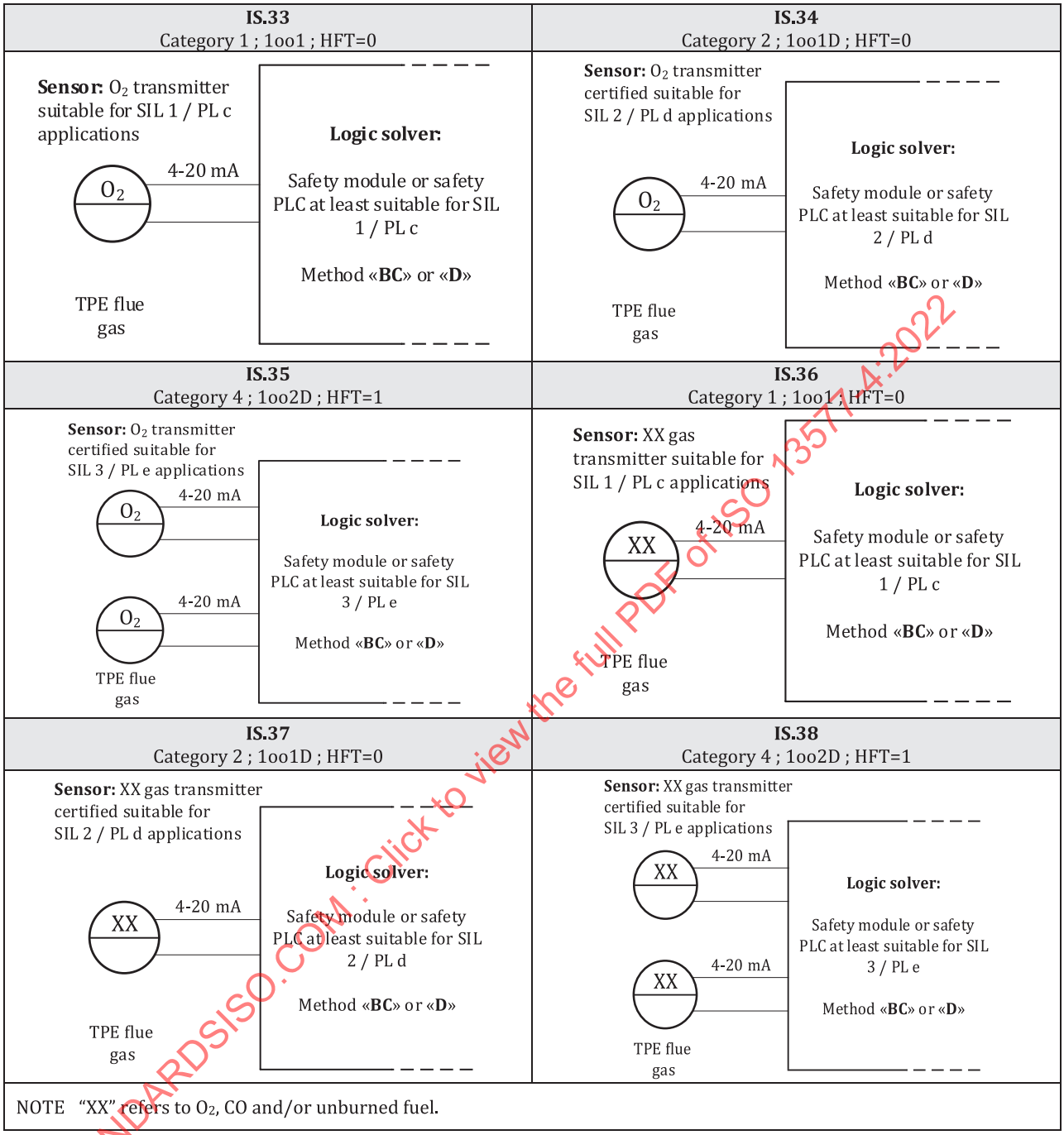


Figure E.6 — Flue gas sensing and status detection

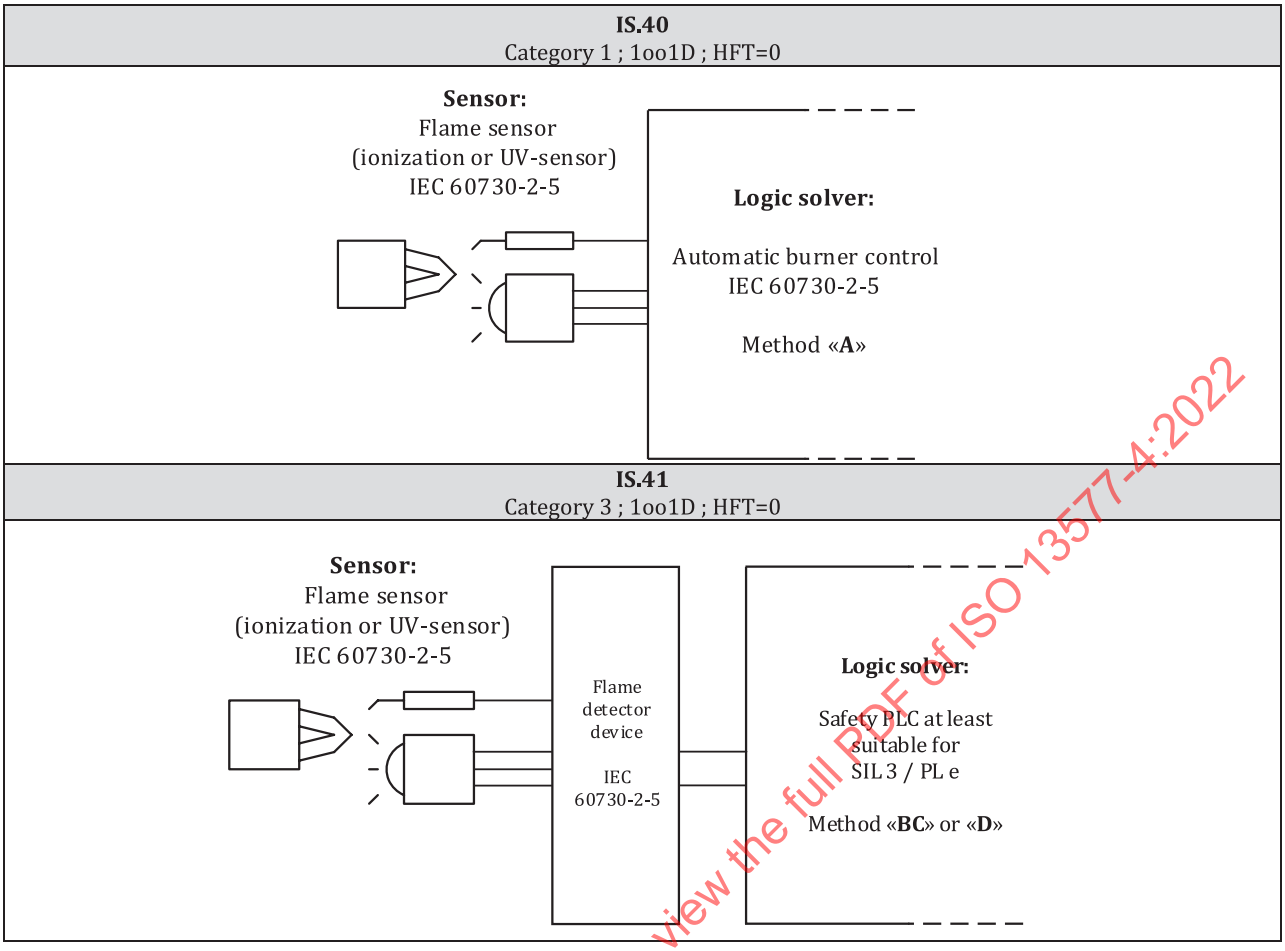


Figure E.7 — Flame sensing and status detection

E.2.2 Overview of different requirements for output subfunctions

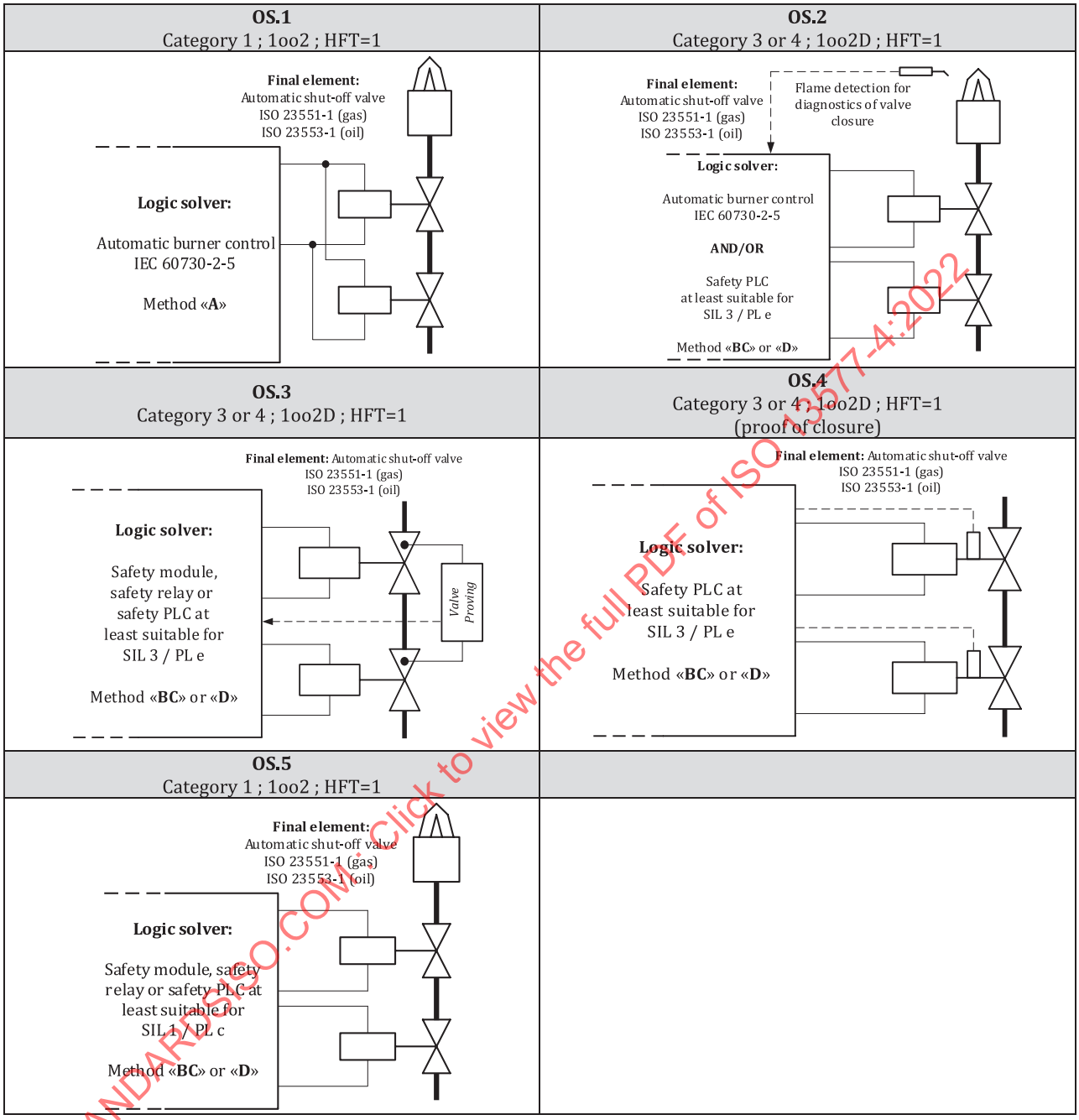


Figure E.8 — Direct fuel command