BS ISO 13577-4:2014

BSI Standards Publication

Industrial furnace and associated processing equipment — Safety

Part 4: Protective systems

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 13577-4:2014.

The UK participation in its preparation was entrusted to Technical Committee RHE/13, Oil burning equipment.

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

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

ISBN 978 0 580 87031 6

ICS 13.100; 25.180.01

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2014.

Amendments issued since publication

Date	Text affected

BS ISO 13577-4:2014

INTERNATIONAL STANDARD

ISO 13577-4

First edition
2014-09-01

Industrial furnace and associated processing equipment — Safety —

Part 4: Protective systems

Fours industriels et équipements associés — Sécurité —

Partie 4: Systèmes de protection

Reference number
ISO 13577-4:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 244, *Industrial furnaces and associated processing equipment*.

ISO 13577 consists of the following parts, under the general title *Industrial furnaces and associated processing equipment — Safety*:

— *Part 1: General requirements*

— *Part 2: Combustion and fuel handling systems*

— *Part 3: Generation and use of protective and reactive atmosphere gases*

— *Part 4: Protective systems*

The following part is under preparation:

— *Part 11: Requirements for arc furnaces*

Introduction

This part of ISO 13577 was developed to specify the requirements of a protective system, which is a safety-related electrical control system (SRECS) of industrial furnaces and associated processing equipment (TPE).

Mandatory safety-related control functions of TPE are specified in ISO 13577-1, ISO 13577-2, and ISO 13577-3.

It is intended that in designing the protective system of TPE, manufacturers of TPE choose from the four methods provided in this part of ISO 13577.

This part of ISO 13577 is to be used together with the other parts of ISO 13577. Since ISO 13577 is a type-C standard of ISO 12100, TPE are required to be designed in accordance with the principles of ISO 12100. However, there are cases in which a risk assessment according to IEC 61511 (all parts) is more suitable for the design of a TPE protective system.

This document is a type-C standard as stated in ISO 12100.

The machinery concerned and the extent to which hazards, hazardous situations, or hazardous events are covered are indicated in the scope of this part of ISO 13577.

When requirements of this type-C standard are different from those which are stated in type-A or -B standards, the requirements of this type-C standard take precedence over the requirements of the other standards for machines that have been designed and built according to the requirements of this type-C standard.

IEC 61511 (all parts) provides the option of a low-demand rate on the protective system. IEC 62061 or ISO 13849-1 always assume high-demand applications.

Therefore, this part of ISO 13577 permits extended risk assessment for SRECS in which risk assessment based on IEC 61511 (all parts) can be chosen as an alternative.

INTERNATIONAL STANDARD **ISO 13577-4:2014(E)**

Industrial furnace and associated processing equipment — Safety —

Part 4: Protective systems

1 Scope

This part of ISO 13577 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 the other parts of ISO 13577.

2 Normative references

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

ISO 13574:—[1)], *Industrial furnaces and associated processing equipment — Vocabulary*

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

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

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

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

IEC 60730-2-5, *Automatic electrical controls for household and similar use — Part 2-5: Particular requirements for automatic electrical burner control systems*

IEC 61508 (all parts):2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

IEC 61511 (all parts), *Functional safety — Safety instrumented systems for the process industry sector*

IEC 62061, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 13574:—[2)] and the following apply.

1) To be published.

2) To be published.

3.1
final element
part of a protective system which implements the physical action necessary to achieve a safe state

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

[SOURCE: IEC 61511-1:2003, 3.2.24 modified: "instrumented system" had 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 signaled

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

[SOURCE: ISO 13574:—[2)], 2.65, modified: The second sentence in the original definition had been presented as in the Note.]

3.3
functional safety
capability of a protective system or other means to reduce risk, to execute the actions required for achieving or maintaining a safe state for the process and its related equipment

[SOURCE: ISO 13574:—[2)], 2.73]

3.4
logic function
function that performs the transformations between input information (provided by one or more input functions or sensors) and output information (used by one or more output functions or final elements)

Note 1 to entry: Logic functions are executed by the logic solver of a protective system.

[SOURCE: IEC 61511-1:2003, 3.2.39, modified — "input functions" had been changed to read "input functions or sensors" and "output function" had been changed to read "output function or final elements" in the definition, and the second sentence in the original definition had been deleted; Note has been added.]

3.5
logic solver
portion of a protective system that performs one or more logic function(s)

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

[SOURCE: IEC 61511-1:2003, 3.2.40 modified: "either a BPCS or SIS" had been changed to read "a protective system" in the definition; Note 1 in the original definition had been deleted.]

3.6
manual reset
action after a lockout of a safety device (e.g. automatic burner control) carried out manually by the supervising operator

[SOURCE: ISO 13574:—[3)], 2.107]

3) To be published.

3.7
performance level
PL
discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions

[SOURCE: ISO 13849-1:2006, 3.1.23]

3.8
product standard
standard for products and devices which are listed in ISO 13577 (all parts) except this part of ISO 13577

[SOURCE: ISO 13574:—[3)], 2.135 modified: "ISO 13577-4" has been changed to read "this part of ISO 13577" in the definition.]

3.9
programmable logic control
PLC
electronic device designed for control of the logical sequence of events

[SOURCE: ISO 13574:—, 2.125]

3.10
protective system
instrumented system used to implement one or more safety-related instrumented functions which is composed of any combination of sensor(s), logic solver(s), and final elements (for example, see Figure 2)

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

[SOURCE: ISO 13574:—, 2.138]

3.11
safety bus
bus system and/or protocol for digital network communication between safety devices, which is designed to achieve and/or maintain a safe state of the protective system in compliance with IEC 61508 (all parts):2010 or IEC 60730-2-5

[SOURCE: ISO 13574:—, 2.164]

3.12
safety device
device that is used to perform protective functions, either on its own or as a part of a protective system

Note 1 to entry: Examples are sensors, limiters, flame monitors, burner control systems, logic systems, final elements, and automatic shut-off valves.

3.13
safety integrity level
SIL
discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest

Note 1 to entry: The target failure measures for the four safety integrity levels are specified in IEC 61508-1:2010, Tables 2 and 3.

Note 2 to entry: Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.

Note 3 to entry: A safety integrity level (SIL) is not a property of a system, subsystem, element, or device. The correct interpretation of the phrase "SIL *n* safety-related system" (where *n* is 1, 2, 3, or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to *n*.

[SOURCE: IEC 61508-4:2010, 3.5.8]

3.14
sensor
device that produces a signal based on a process variable

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

3.15
system for permanent operation
system, which is intended to remain in the running position for longer than 24 h without interruption

[SOURCE: IEC 60730-2-5:2009, 2.5.101]

3.16
system for non-permanent operation
system, which is intended to remain in the running position for less than 24 h

[SOURCE: IEC 60730-2-5:2009, 2.5.102]

3.17
systematic capability
measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element

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

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

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

[SOURCE: ISO 13574:—, 2.183]

4 Design requirements for equipment in a protective system

4.1 General

Electrical equipment shall comply with IEC 60204-1 and withstand the hazards identified in the risk assessment required at the design stage. Electrical 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 the manufacturer's instructions including safety manuals. Any device used outside of its published technical specification shall be verified and validated to be suitable for the intended application.

Devices of a protective system shall withstand the environmental conditions and fulfill 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.

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

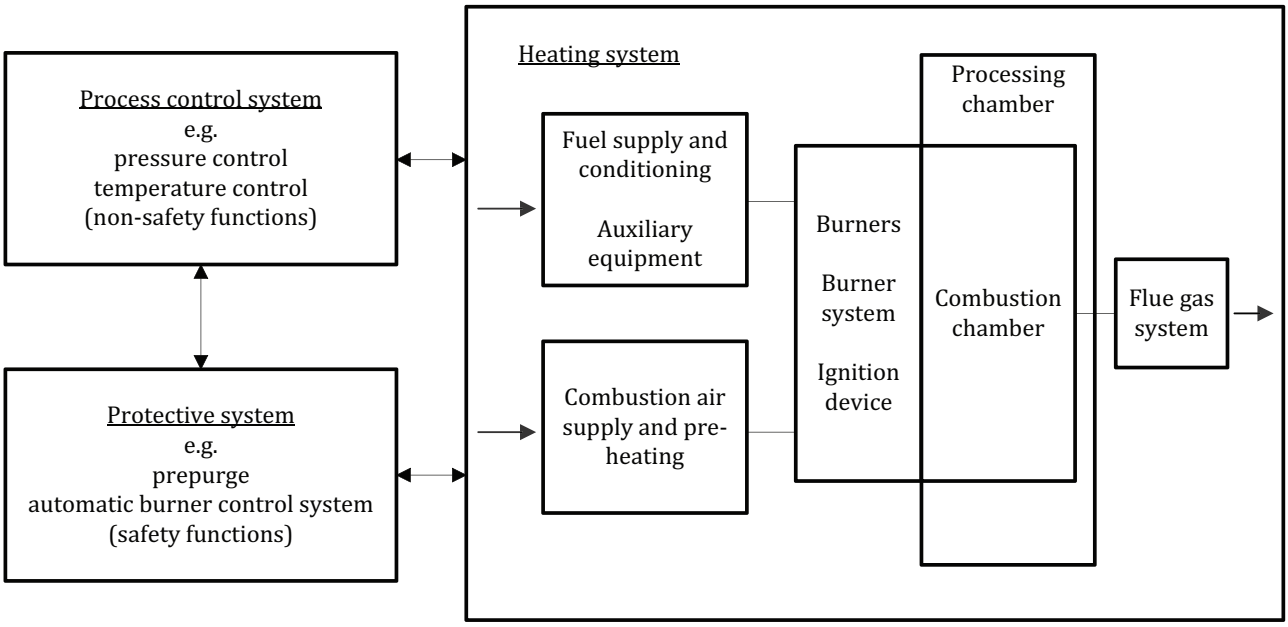


Figure 1 — Block diagram of control and protective systems

An appropriate group of techniques and measures shall be used that are designed to prevent the introduction of 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 Annex B).

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 y.

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

4.2 Requirements for protective systems

Any one or a combination of the four (4) methods shall be used to implement a protective system for the safety function(s) requirements identified in ISO 13577 (all parts); however, only one method shall be used for any one specific safety function. The four methods are the following:

— Method A as specified in 4.2.1;

— Method B as specified in 4.2.2;

— Method C as specified in 4.2.3;

— Method D as specified in 4.2.4.

Figure 2 shows the basic configuration of a protective system.

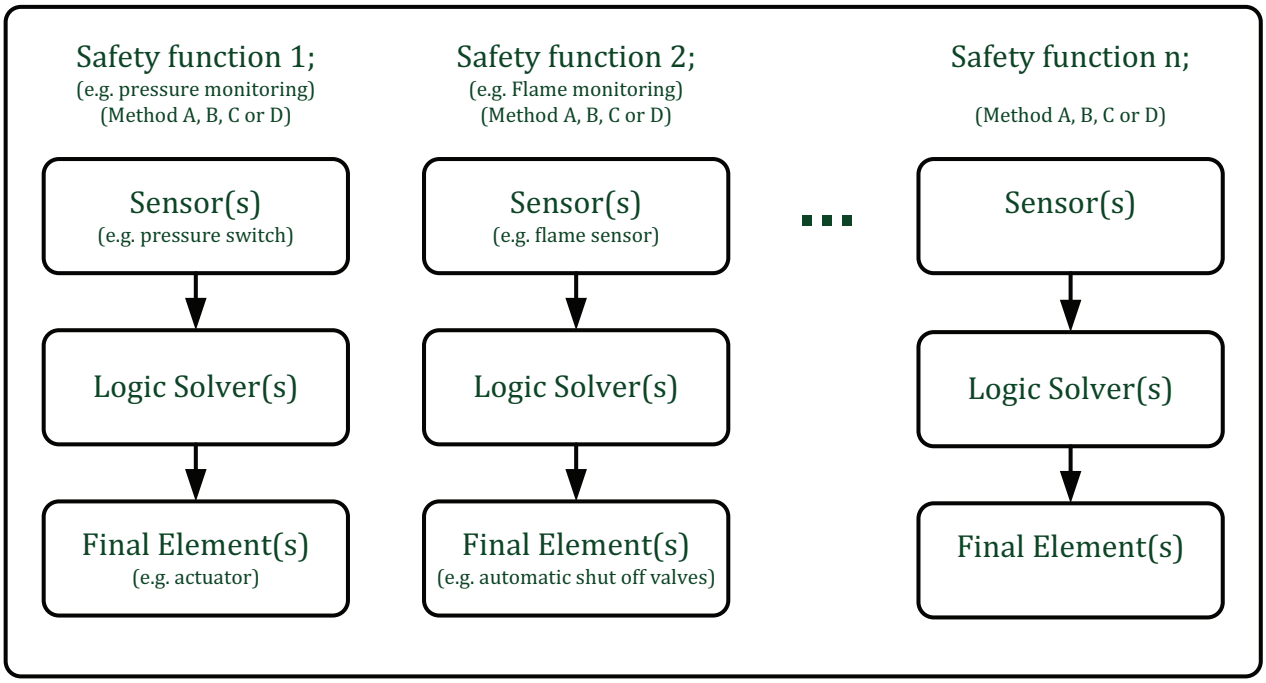


Figure 2 — Basic configuration of a protective system

Figure 3 shows the basic characteristics of each method.

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

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

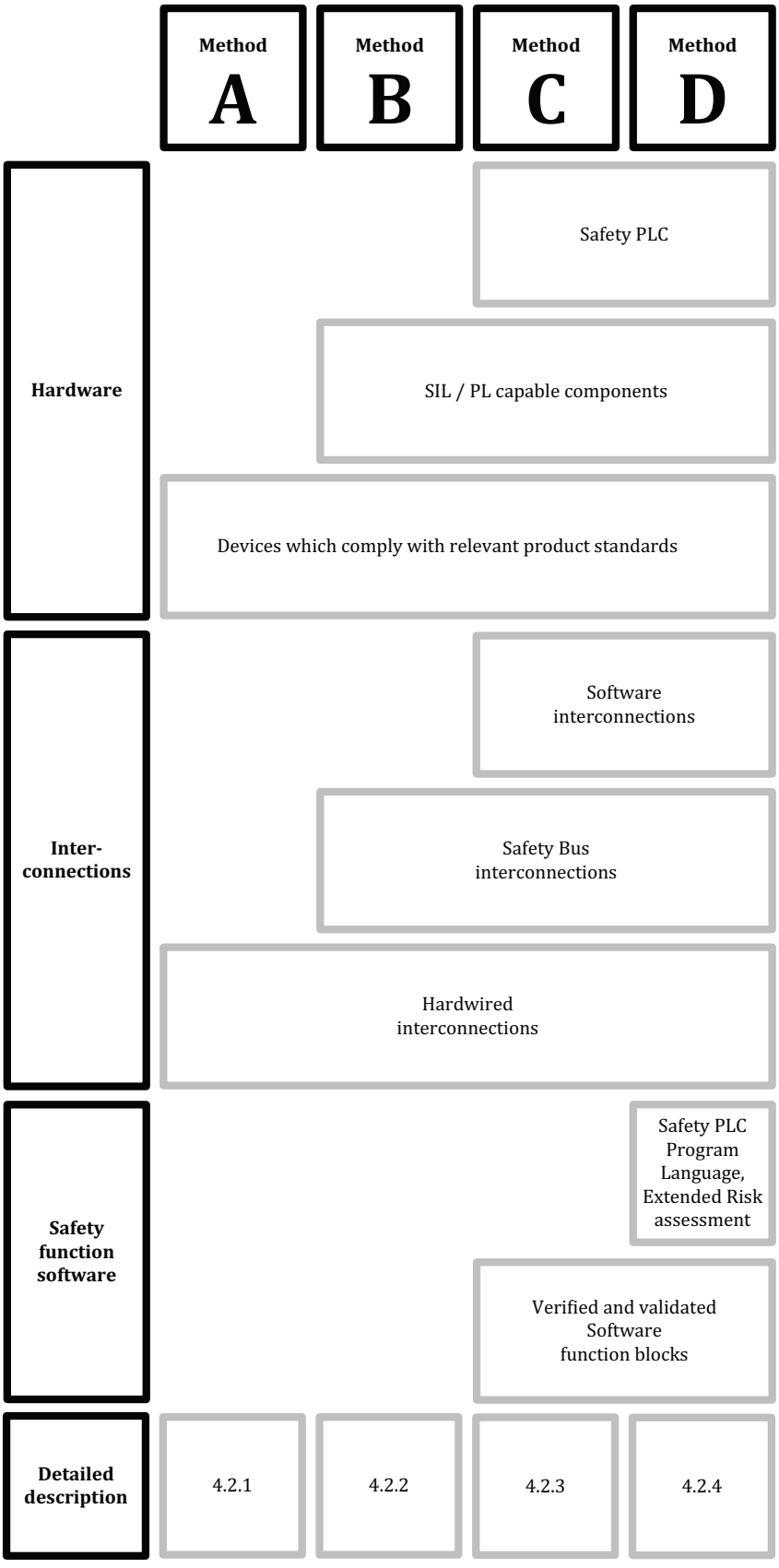


Figure 3 — Method overview

See Annex E for sample schematic diagrams of the various methods.

4.2.1 Method A

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

The requirements of IEC 61508 (all parts), IEC 61511 (all parts), IEC 62061, and ISO 13849-1:2006 are not applicable for this type of protective system.

The following requirements for hardwiring shall be fulfilled:

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

— connections shall not be permitted through data communication buses;

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

— hardwiring shall be in accordance with Annex F.

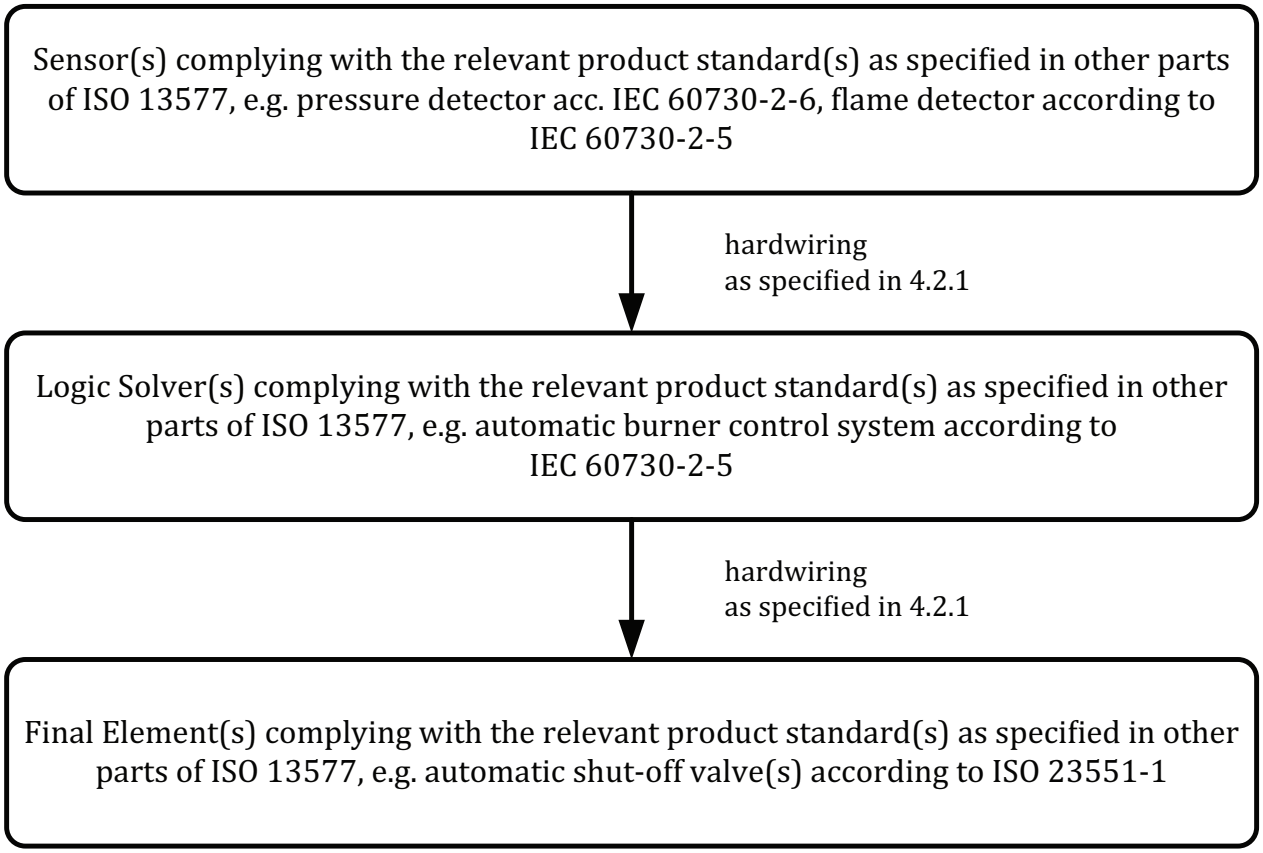


Figure 4 — Hardware configuration of Method A

NOTE The safety devices used in 4.2.1 correspond to specific safety requirements, matched to the field of application and the functional requirements made of these devices, as demanded in the corresponding products 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 4.2.1 is one of several alternative methods.

4.2.2 Method B

Method B shall be a combination of devices meeting the relevant product standards and/or SIL/PL capable devices for which no relevant product standard exits. Safety PLCs are excluded (see Figure 5).

The following requirements for hardwiring shall be fulfilled:

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

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

— interconnections may be hardwired or through safety bus;

— hardwiring shall be in accordance with Annex F.

For devices which are not covered by product standards, the following requirements shall be fulfilled:

— the device shall be SIL 3 capable in accordance with IEC 61508 (all parts), IEC 62061, or IEC 61511 (all parts) or it shall be PL e capable in accordance with ISO 13849-1:2006;

— SIL/PL capability certification shall apply to the complete device, including the hardware and software.

NOTE Verification and validations of SIL/PL certification for devices is typically carried out by a notified body, accredited national testing laboratory, or by an organization in accordance with ISO/IEC 17025:2005.

Devices with less than SIL 3/PL e capability shall be permitted, provided the SIL/PL requirements for the loop (safety function) are determined and calculated.

When the SIL is determined by prior use (i.e. proven in use), the requirements in IEC 61511 (all parts) shall be followed.

All requirements in the safety handbook for the device shall be adhered to, such as the proof test interval.

NOTE See Annex C for examples of determining SIL/PL.

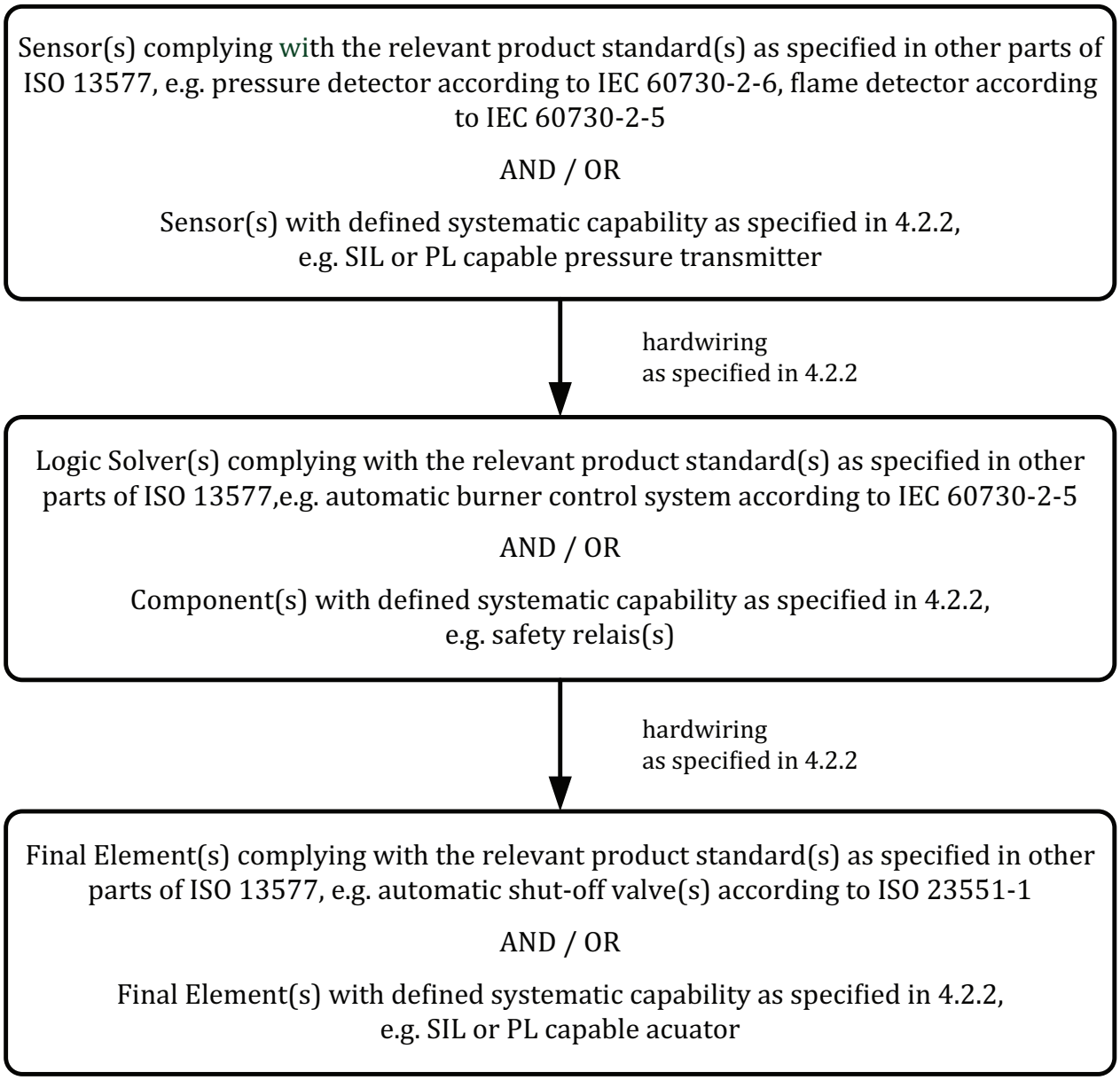


Figure 5 — Hardware configuration of Method B

4.2.3 Method C

Method C shall be a combination of devices meeting the relevant product standards and/or SIL/PL capable devices for which no relevant product standard exits and/or safety PLCs.

The following requirements for hardwiring shall be fulfilled:

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

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

— the interconnections may be hardwired, through safety bus, or through software interconnections;

— hardwiring shall be in accordance with Annex F.

Safety function software is only permitted in the form of verified and validated SIL 3 capable software function blocks (see Figure 6).

Safety functions shall be permitted within a safety-rated device (e.g. a safety PLC) 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:

— the devices shall be SIL 3 capable in accordance with IEC 61508 (all parts), IEC 62061, or IEC 61511 (all parts) or it shall be PL e capable in accordance with ISO 13849-1:2006;

— 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;

— software interconnections in a programmable device shall be verified by a functional test;

— software programming languages for PLCs shall be in accordance with IEC 61131-3;

— software shall be locked and secured against unauthorized and unintentional changes.

NOTE Verification and validations of SIL/PL certification is typically carried out by a notified body, accredited national testing laboratory, or by an organization in accordance with ISO/IEC 17025:2005.

Devices with less than SIL 3/PL e capability shall be permitted, provided the SIL/PL requirements for the loop (safety function) are determined and calculated.

When the SIL is determined by prior use (i.e. proven in use), the requirements in IEC 61511 (all parts) shall be followed.

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

NOTE See Annex C for examples of determining SIL/PL.

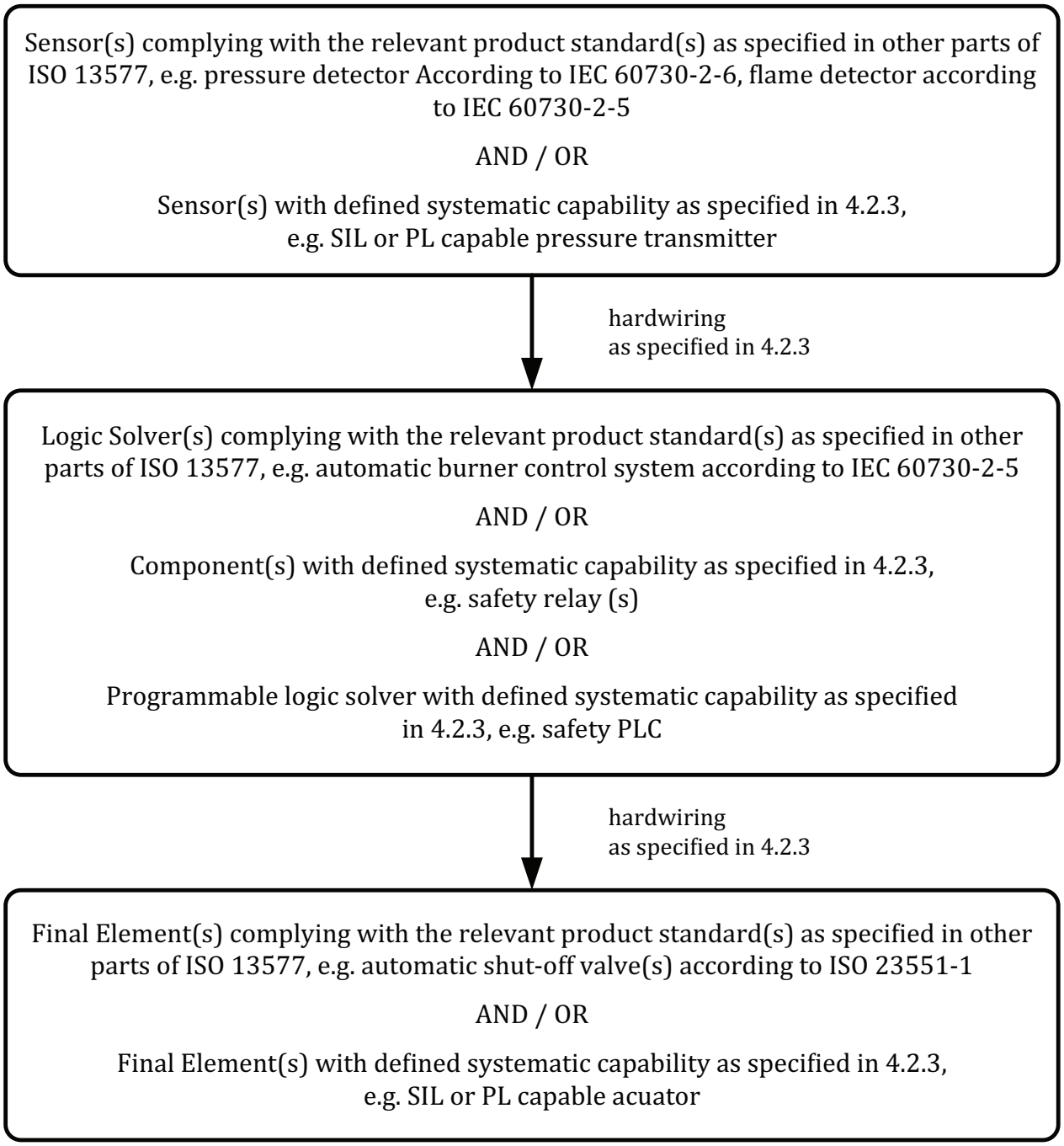


Figure 6 — Hardware configuration of Method C

4.2.3.1 Requirements for application software

4.2.3.1.1 In accordance with the required safety integrity level, the chosen programmable protective equipment and its software shall meet the safety integrity requirements of the particular application:

— correctness of functionality;

— sequencing and time-related information;

— timing constraints;

— concurrency (software interrupts should be avoided);

— data structures and properties;

— design assumptions and dependencies;

— testability.

4.2.3.1.2 The proof of the items listed in 4.2.3.1.1 has to be carried out by verification and validation steps according to the design and development phases within the life cycle of the software, including

— validity of the software requirement specification and

— completeness, consistency, understandability, and unambiguousness of documentation and programs.

The application design representations shall be based on a notation (e.g. functional diagram), which is unambiguously defined or restricted to unambiguously defined features; as far as practicable, the application design shall minimize the safety-related part of the software. Where the software is to implement both safety and non-safety functions then all of the software shall be treated as safety-related, unless adequate independence between the functions can be demonstrated in the application design. Where the software is to implement safety functions of different safety integrity levels, then all of the software shall be treated as belonging to the highest safety integrity level unless adequate independence between the safety functions of the different safety integrity levels can be shown in the application design. The justification for independence shall be recorded in the relevant design documentation.

If software modules proven in operation are to be used as part of the application software, they shall be clearly identified and documented. The software's suitability in satisfying the requirements of a particular application shall be justified. Suitability shall be based upon evidence of satisfactory operation in a similar application or having been subject to the same verification and validation procedures as would be expected for any newly developed software. For software modules proven in operation, the extent of testing may be limited to the tests required to ensure proper implementation. Constraints from the previous software environment (e.g. operating system and compiler dependencies) should be evaluated. Depending on the nature of the software development, responsibility for conformance with 4.2.3.1 can vary from the supplier alone, the user alone, or both. The division of responsibility shall be recorded. The proposed software architecture shall be based on a partitioning into devices/subsystems, which can be identified to be part of the system software and of the plant-specific application software.

The following information shall be provided:

— whether they are new, existing, or proprietary;

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

— whether each subsystem/device is safety-related or not;

— the software safety integrity level of the subsystem/device;

— identification, evaluation, and details of the significance of all hardware/software interactions;

— a notation used to represent the architecture which is unambiguously defined or restricted to unambiguously defined features;

— identification of the design features used for maintaining the safety integrity of all data (this shall include plant input-output data, communications data, operator interface data, maintenance data, and internal database data).

4.2.4 Method D

Method D shall be in accordance with the full requirements of IEC 61508 (all parts), IEC 62061, IEC 61511 (all parts), or ISO 13849-1:2006 (see Figure 7).

NOTE See Annex D for the method in accordance with IEC 61511 (all parts).

Method D shall also fulfill the following requirements:

a) the flame detector device shall comply with IEC 60730-2-5;

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

c) each functional safety requirement, as identified in ISO 13577 (all parts), shall be evaluated for its need in accordance with the standards, such as IEC 61511 (all parts), ISO 13849-1:2006, and IEC 62061, and implemented with the required SIL for each function. Safety functions of the safety-related system, such as automatic burner control, valve proving, air/fuel ratio control, etc. shall fulfill the intent of the safety requirements in the relevant product standards;

NOTE An extended risk assessment in Method D can take precedence over the safety requirements in ISO 13577 (all parts). By nature of the extended risk assessment under Method D, the overall safety is not reduced and meets or exceeds the intended requirements of ISO 13577 (all parts).

d) the interconnections may be hardwired, through safety bus, or through software interconnections;

e) hardwiring shall be in accordance with Annex F.

NOTE Verification and validations of SIL/PL certification is typically carried out by a notified body, accredited national testing laboratory, or by an organization according to ISO/IEC 17025:2005.

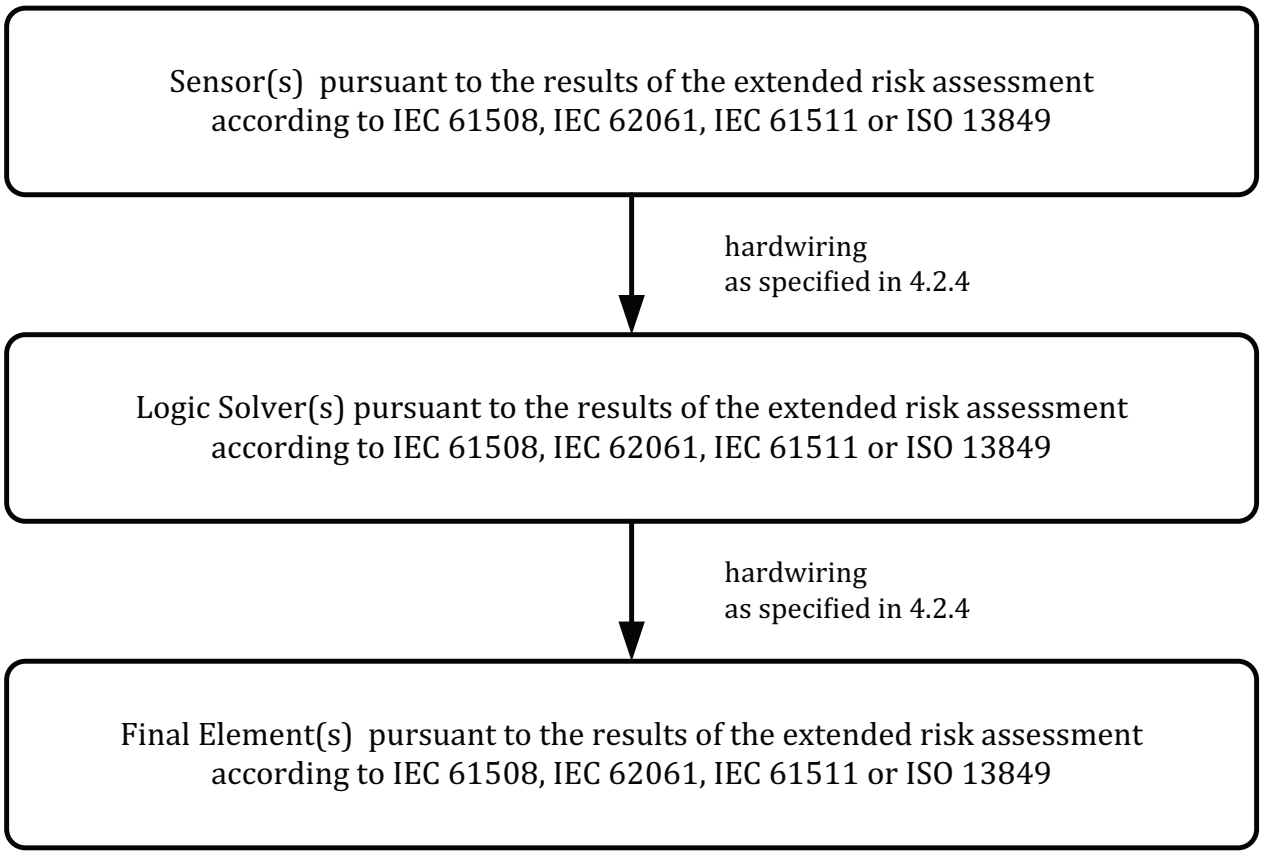


Figure 7 — Hardware configuration of Method D

4.3 Fault assessment for the hardwired section of protective systems

The protective system shall be designed such that the devices required in ISO 13577 (all parts) shall be used as follows:

a) When relays are used in safety functions, the contacts shall be supervised and forced guided 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 or the requested SIL/PL requirement. Power relays for safety with or without mirror contacts shall be in accordance with IEC 60947-4-1 or the requested SIL/PL requirement.

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

c) For Methods B and C, when timers not complying with the relevant product standards as specified in all the other parts of ISO 13577 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.

e) Additional requirements are given in Annex F.

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:—, 4.2.7 or 4.3.7).

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:—, 2.107).

A reset 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 based on the risk assessment and shall be specified in the instruction handbook.

When the manual reset is initiated without visible sight on the TPE, a safe operation shall be ensured from the reset action and the actual status and relevant information of the process under control shall be visible to the user.

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.

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.

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 and 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 developer's 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 its lifecycle.

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

Plan the protective system integration tests and for the test plan documentation, including the following:

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

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

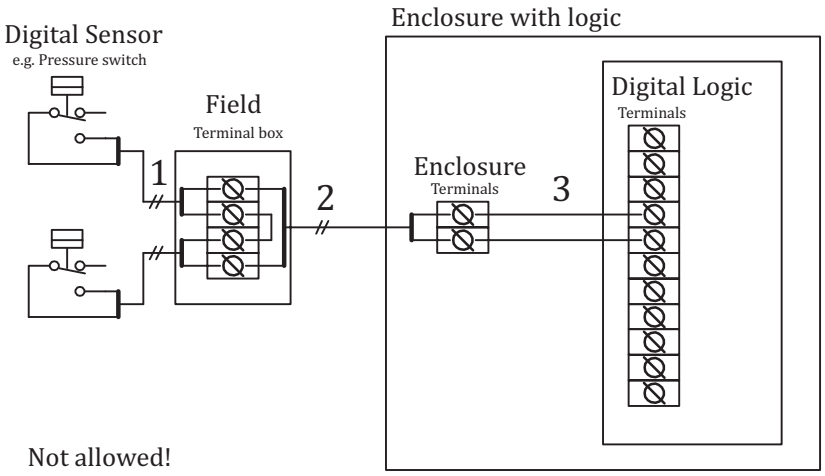
c) the pass/fail criteria.

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

Annex B
(informative)

Examples of techniques for avoiding failures from external wiring

Figure B.1 shows how a possible short circuit at cable 2 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 at cable 2, the open state of either switch is not detected.



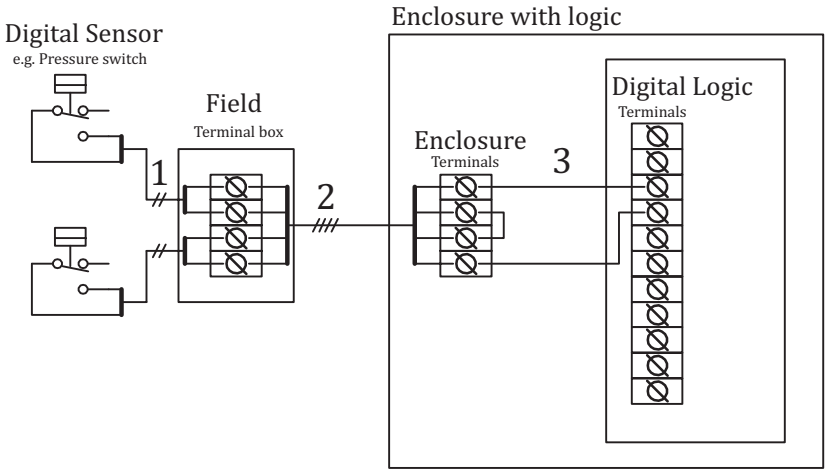
Key

1 cable 1
2 cable 2
3 cable 3

Figure B.1 — Improper external wiring method

CAUTION — Figure B.1 shows an IMPROPER example of external wiring practice.

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 and B. All conductors are brought back to the main enclosure through cable ducts or conduits, which provide sufficient protection from mechanical and thermal damage. Also, the interconnecting wire links are made within the main enclosure of the protective system logic solver.



Key

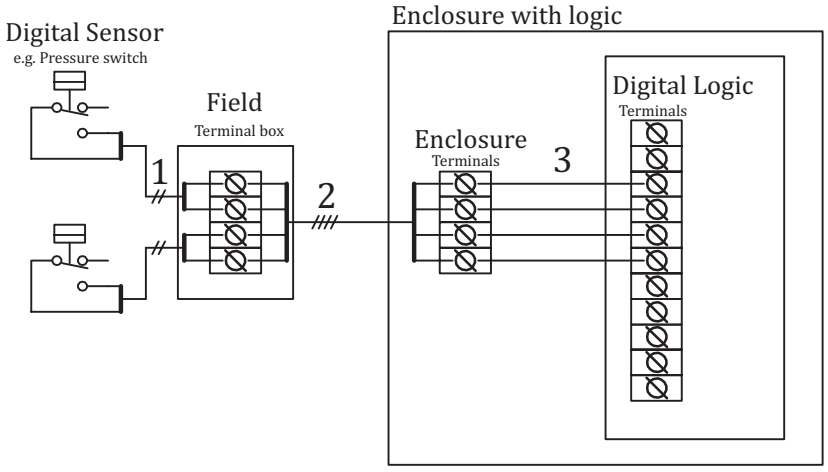
1 cable 1

2 cable 2

3 cable 3

Figure B.2 — Protected wiring

Figure B.3 shows a slight variation of Figure B.2 where the protective system device accepts each conductor from the sensors and can provide a sufficient level of protection for the safety function when using any of the protective system methods, A, B, C, or D.



Key

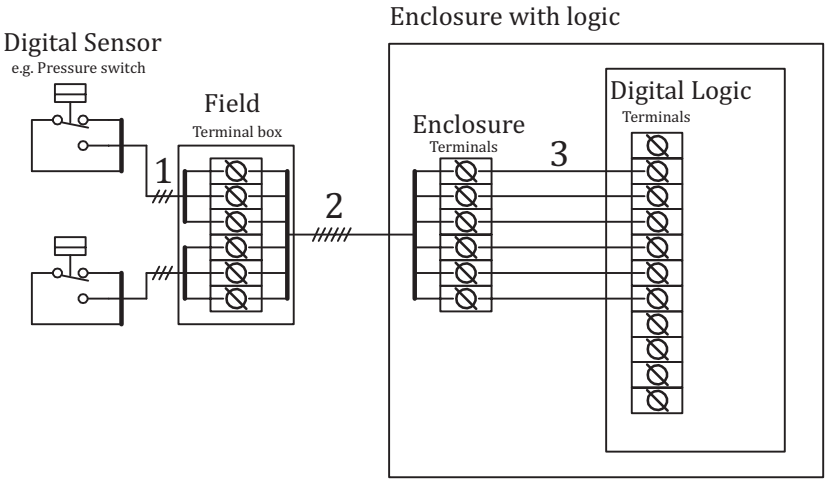
1 cable 1

2 cable 2

3 cable 3

Figure B.3 — Protected wiring, all conductors carried throughout

Figure B.4 shows a technique where both states of the sensor switch is 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, B, C, or D.

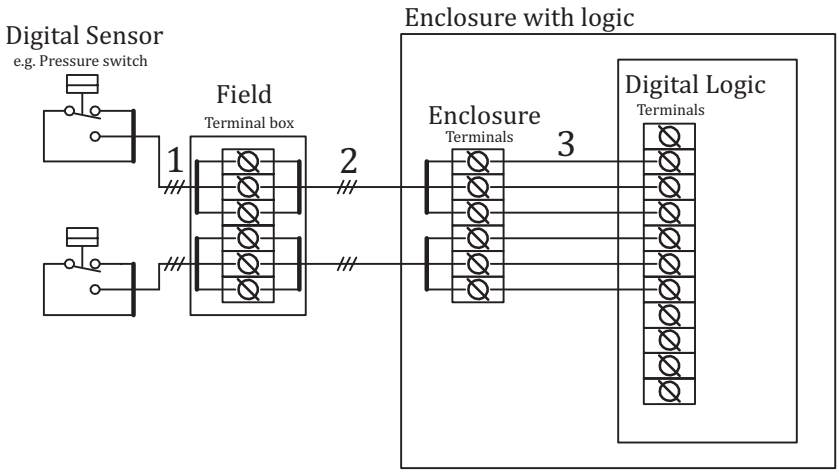


Key

1 cable 1
2 cable 2
3 cable 3

Figure B.4 — Supervising both states

Figure B.5 shows a variation of Figure B.4 where the 6-conductor single cable 2 could be replaced with two 3-conductor cables.

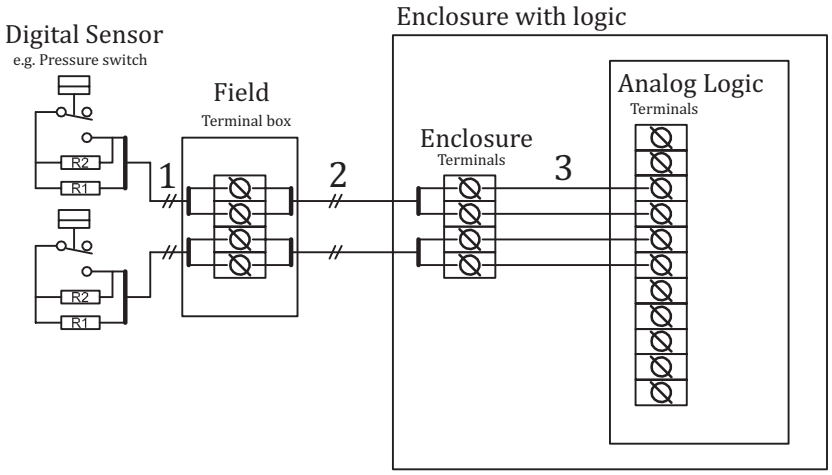


Key

1 cable 1
2 cable 2
3 cable 3

Figure B.5 — Supervising both states, multiple cables

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



Key

1 cable 1
2 cable 2
3 cable 3

Figure B.6 — Supervision by analog value

Annex C
(informative)

Examples for the determination of safety integrity level SIL using the risk graph method

C.1 General

Several International Standards can be used for determination of the required SIL/PL. For machinery, IEC 62061 was developed to determine the SIL while IEC 61511(all parts):—[4] 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 and IEC 61511 (all parts):—[4]]. In addition, ISO 13849-1:2006 covers the determination of a performance level PL and also includes a method to determine PL from SIL (ISO 13849-1:2006, Table 4).

A hazard and risk analysis shall 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:

— consequences of the hazardous event (parameter Se in accordance with Annex A of IEC 62061, parameter C in accordance with IEC 61511-3:—[4]); the worst case scenario shall be taken into account;

— frequency and duration of the time spent in the hazardous area (parameter Fr in accordance with Annex A of IEC 62061, parameter F in accordance with IEC 61511-3); the factor of time spent must 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;

— possibility of preventing or avoiding the hazardous event (parameter Av in accordance with Annex A of IEC 62061, parameter P in accordance with IEC 61511-3:—[4]);

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

Parameter Av in accordance with Annex A of IEC 62061 and parameter P in accordance with IEC 61511-3:—[4] 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

— 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, and

— 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.

---

4) The edition 2 of IEC 61511 (all parts) is under development and is to be issued in 2015.

Parameter Pr in accordance with Annex A of IEC 62061 and parameter W in accordance with IEC 61511-3:—[5)] 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 the decisions made and grounds must be documented in writing.

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 SIL/PL determination under different risk environment in accordance with Annex A of IEC 62061/ISO 13849-1:2006, Table 4.

C.2.2 Example 2 – Table C.2

Table C.2 shows a comparison of SIL/PL determination under different risk environment Example of SIL determination in accordance with IEC 61511-3:—[5)].

5) The edition 2 of IEC 61511 (all parts) is under development and is to be issued in 2015.

Table C.1 — Comparison of SIL/PL determination under different risk environment in accordance with IEC 62061 and ISO 13849-1:2006, Table 4

Risk assessment and safety measures									Document No.: Part of:				
Project: Example of typical SIL determination													
Issued by:									☐ Pre risk assessment				
Date:									☐ Intermediate risk assessment				
Revision:									☐ Follow up risk assessment				
			Black area = Safety measures required Grey area = Safety measures recommended										
	Consequences	Severity	Class Cl					Frequency and		Probability of hzd.		Avoidance	
		Se	3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	duration, Fr		event, Pr		Av	
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

Table C.1 *(continued)*

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 sensor 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:—, 4.2.2.6/4.3.2.8, Automatic shut-off valves Hazard: fire, mechanical breakdown, injuries from hot parts
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature sensor 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:—, 4.2.2.6/4.3.2.8, Automatic shut-off valves Hazard: fire, mechanical breakdown, injuries from hot parts
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature sensor 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:—, 4.2.2.6,/4.3.2.8, Automatic shut-off valves Hazard: fire, mechanical breakdown, injuries from hot parts
12	Combustion air pressure/ flow too low	Pressure switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2, Air flow and pressure detectors Hazards: explosion, fire, poisoning, incomplete combustion
NOTE For guidance of this risk graph, see C.2.3.											

Table C.1 *(continued)*

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**	
12	Combustion air pressure/ flow too low	Pressure switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2, Air flow and pressure detectors Hazards: explosion, fire, poisoning, incomplete combustion
12	Combustion air pressure/ flow too low	Pressure switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2: air flow and pressure detectors 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:—, 4.2.3.3/4.3.3.3: Air/fuel ratio, 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	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:—, 4.2.3.3/4.3.3.3: Air/ fuel ratio Hazard: explosion, fire, poisoning.
NOTE For guidance of this risk graph, see C.2.3.											

Table C.1 *(continued)*

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**	
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:—, 4.2.3.3/4.3.3.3: Air/fuel ratio Hazard: explosion, fire, poisoning.
NOTE For guidance of this risk graph, see C.2.3.											

Table C.2 — Comparison of SIL/PL determination under different risk environment in accordance with IEC 61511

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 must 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.			Estimated SIF demand rate			W
			Likelihood sum (F+P+W)													W_9	Often	>1/ y	9
Severity level		C	1-2	3-4	5-6	7-8	9-10	11-12					Conditions to be fulfilled:			W_8	Frequent	1/1-3 y	8
C_F	Catastrophic	F	a	SIL 1	SIL 2	SIL 3	SIL 4	b								W_7	Likely	1/3-10 y	7
C_E	Extensive	E	OK	a	SIL 1	SIL 2	SIL 3	SIL 4	Exposure rate			F	•Facilities to alert operator that the SIS has failed			W_6	Probable	1/10-30 y	6
C_D	Serious	D	OK	OK	a	SIL 1	SIL 2	SIL 3	F_D	Permanent	100 %	2	•Independent facilities to bring process to safe state			W_5	Occasional	1/30-100 y	5
C_C	Considerable	C	OK	OK	OK	a	SIL 1	SIL 2	F_C	Frequent	10 % –100 %	2	•Time between operator alert and hazardous event >1h			W_4	Remote	1/100-300 y	4
C_B	Marginal	B	OK	OK	OK	OK	a	SIL 1	F_B	Occasionally	1 % – 10 %	1	Avoidance probability		P	W_3	Improbable	1/300-1000 y	3
C_A	Negligible	A	OK	OK	OK	OK	OK	a	F_A	Rare	<1%	0	P_B	Avoidance condition not fulfilled	1	W_2	Incredible	1/1000-10000 y	2
													P_A	All avoidance conditions are fulfilled	0	W_1	Inconceivable	1/10000-100000 y	1

Table C.2 *(continued)*

SIF	Hazardous event	Safety instrumental function (SIF)	Consequences		Influence		Demand	Likelih.	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 sensor 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:—, 4.2.2.6/4.3.2.8: Automatic shut-off valves Hazard: fire, mechanical breakdown injuries from hot parts
			E	B	1	0		7	—		
			F	D				7	1		
10	Plant temperature exceeding the maximum allowable operating temperature	A temperature sensor 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:—, 4.2.2.6/4.3.2.8: Automatic shut-off valves 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 sensor 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:—, 4.2.2.6/4.3.2.8: Automatic shut-off valves 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 switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2: Air flow and pressure detectors Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	0		7	—		
			F	E				7	2		
12	Combustion air pressure/flow too low	Pressure switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2: Air flow and pressure detectors Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	1		8	—		
			F	E				8	2		

Table C.2 *(continued)*

SIF-	Hazardous event	Safety instrumented function (SIF)	Consequences		Influence		Demand	Likelih.	Integrity		Hazard description
No.	Description	Description	Harm	C	F	P	W	Sum	SIL	**SIL**	and comments
12	Combustion air pressure/ flow too low	Pressure switch, pressure transmitter or flow meter 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:—, 4.2.3.2/4.3.3.2: Air flow and pressure detectors Hazards: explosion, fire, poisoning, incomplete combustion
			E	B	1	1		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	1	0	7	8	1	**2**	Minor consequences for few people who have a good chance to escape in time ISO 13577-2:—, 4.2.3.3/4.3.3.3: Air/ fuel ratio 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:—, 4.2.3.3/4.3.3.3: Air/ fuel ratio Hazard: explosion, fire, poisoning.
			E	B	1	1		9	a		
			F	E				9	3		
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:—, 4.2.3.3/4.3.3.3: Air/ fuel ratio 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 Annex A of IEC 62061 ed1.1:2012 (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

  — frequency and duration of the exposure of persons to the hazard, Fr,

  — probability of occurrence of a hazardous event, Pr, and

  — possibilities to avoid or limit the harm, Av.

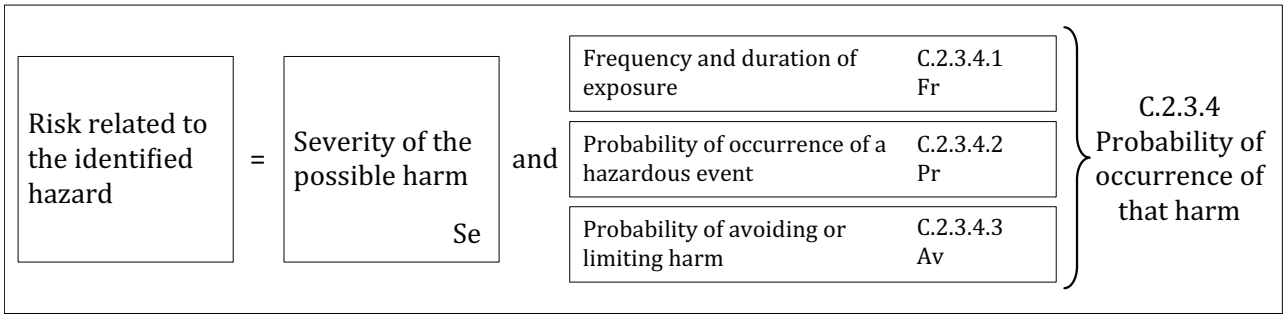


Figure C.1 — Parameters used in risk estimation

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

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.

NOTE 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 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 y	3
>1 y	2

C.2.3.4.2 Probability of occurrence of a hazardous event

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 SRECS. This is necessary in order to estimate the amount of risk that will be exposed if the SRECS fails. In general terms, it must 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 1 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 SRECS 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.

   NOTE 2 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)	
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:—[6](i.e. Table C.2)

The risk graph matrix in accordance with IEC 61511-3:—[6] 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 (SIF) is the maximum determined integrity level.

C.2.4.1 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 hazards (*F*). 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				

6) The edition 2 of IEC 61511 (all parts) is under development and is to be issued in 2015.

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 effecting 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.
NOTE C: Severity level					

Table C.11 *(continued)*

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.2.4.2 Occupancy parameter selection

Occupancy parameter represents 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 (F_D) shall be chosen. Exposure rate F_C shall be chosen if occupancy is frequent or if the occupancy is dependent on the hazardous situation. Exposure rate F_B should be chosen if the area is occupied just occasionally and human presence is obviously independent of the hazardous situation. Exposure rate F_A 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.2.4.3 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 P_B "Avoidance conditions not fulfilled". P_A 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. P_A could also be claimed if the hazardous event is likely avoided in time by manual operator actions. In this case, P_A 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 P_A, and 1 h is a minimum requirement between operator alert and the hazardous event for taking credit for "Possibility of avoidance" (P_A). Fill in the correlating number (0 or 1) of the selected avoidance parameter in the P column.

C.2.4.4 Demand rate parameter selection

Demand rate parameter represents 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 IEC 61511 (all parts):—[7] (risk reduction factor >0,1). Fill in the chosen number correlating to the estimated or calculated residual demand rate in column W.

C.2.4.5 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.

7) The edition 2 of IEC 61511 (all parts) is under development and is to be issued in 2015.

Annex D
(informative)

Example of an extended risk assessment for one safety instrumented function using the IEC 61511 method

D.1 General

The following provides a partial example of the procedures that are used when designing a system in accordance with IEC 61511 (all parts):2003 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 4-20 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 off line for maintenance.

The control valve is a motor operated butterfly valve with a line voltage powered actuator. The control signal is 4-20 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:

a) 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 buildup 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.

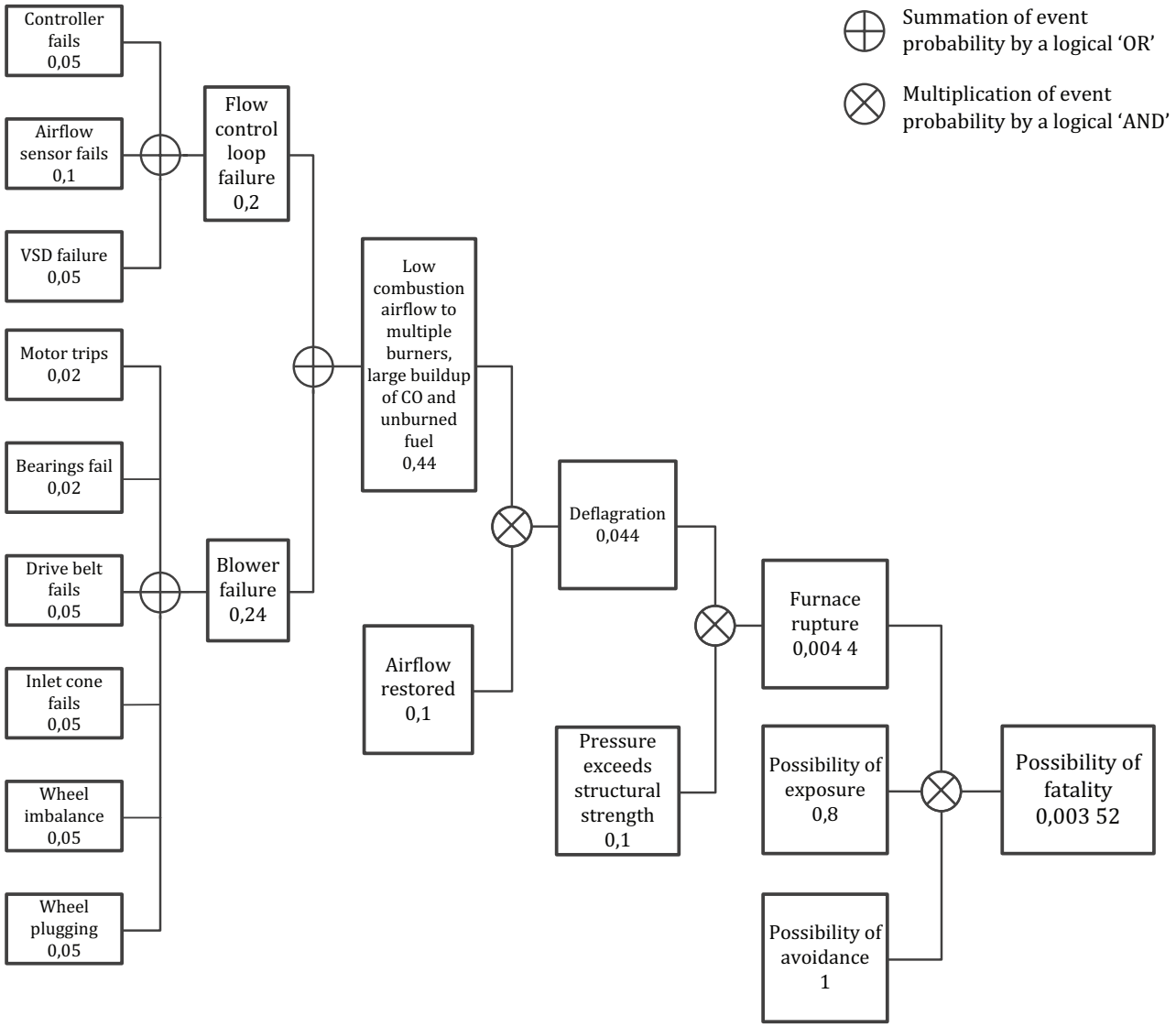


Figure D.1 — Event tree example

D.6 Protective system safety requirement specification

NOTE This section 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 airflow 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 airflow 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 y 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 must provide 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 shutoff valves shall be fail closed.

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

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 shutoff 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 y for each safety function.

l) The safety function shall be proof tested with 90 % coverage each 2 y. 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[8)] providing a hardware fault tolerance of 1.

— 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.

8) 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, Annex B.

— 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 IIA 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 analog 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 y without recalibration,

  k) be factory calibrated with a traceable calibration certificate,

  l) have a systematic capability of SIL 3,

  m) be provided with a suitable SIL certificate, and

  n) be wired using 1,5 mm2 twisted, shielded pair armoured instrument cable with the drain bonded at the logic solver side [the cable shall be run in 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

  a) continuously rise with no low points or sags (the sensing lines shall be self draining to the combustion airflow duct),.

  b) be a minimum of 12 mm to ensure a fast response without dampening, and

  c) be the same length for all sensor connections to ensure similar transportation lag time,

— 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.

  a) 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 comparision and HMI

— Each flow sensor with the 1oo2D pair shall be wired to separate 4 mA to 20 mA 12 bit isolated loop powered analog 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 restore (MTTR) for the 1oo2D function is assumed to be 72 h.

— 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 O2 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 airflow 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 on-line 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 litres/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 y.

D.6.6 Startup requirements

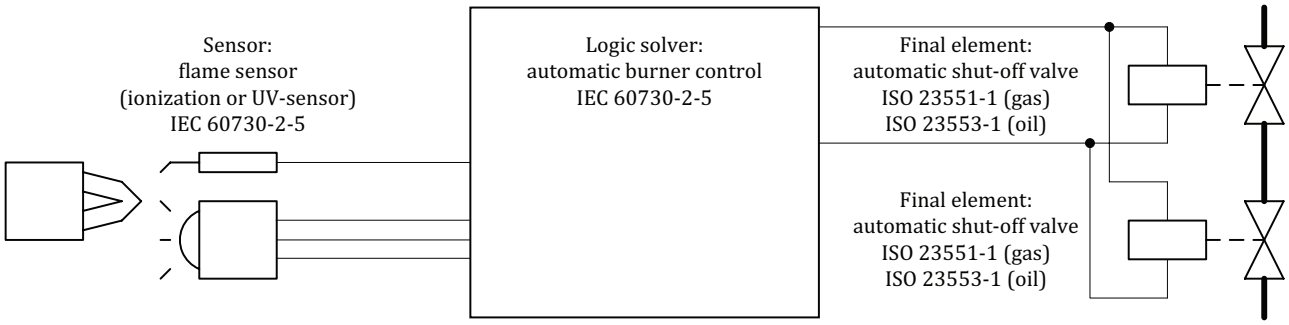
The combustion air blower is in operation when the ESD button is not de-energized and the blower disconnect is set to On. There should therefore be combustion airflow at all times and there is no requirement to bypass the combustion airflow during startup.

During the purge, the combustion airflow 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 airflow 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)

Sample schematic diagrams of protective system

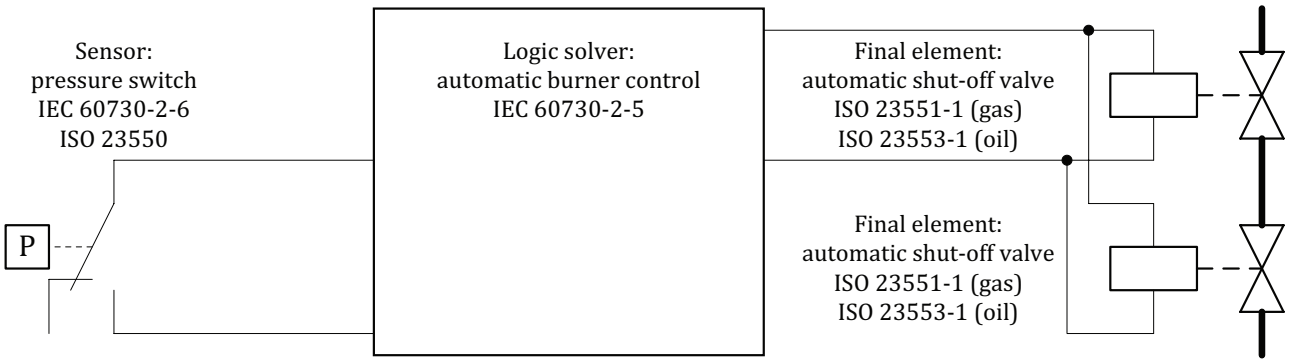
Figures E.1 through E.18 shows sample schematic diagrams of the various methods.



NOTE 1 This figure shows an example of the application of 4.2.1 Method A.

NOTE 2 Safety function: flame monitoring.

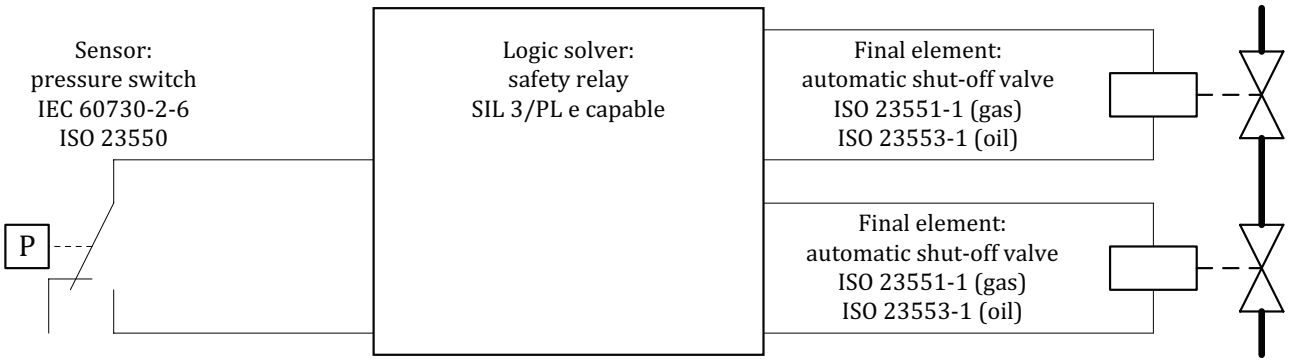
Figure E.1



NOTE 1 Example for when applying 4.2.1 Method A.

NOTE 2 Safety function: minimum pressure monitoring.

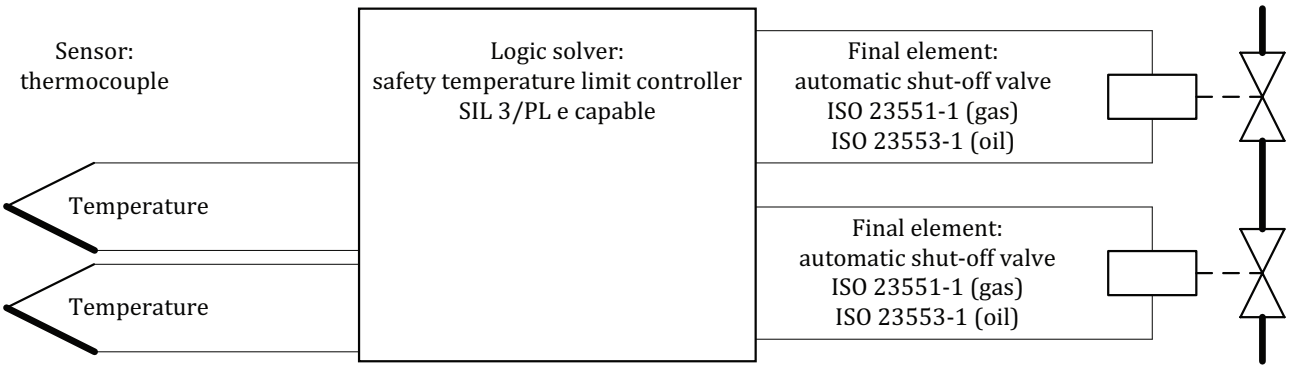
Figure E.2



NOTE 1 This figure shows one loop as an example for when applying 4.2.2 Method B.

NOTE 2 Safety function: minimum pressure monitoring.

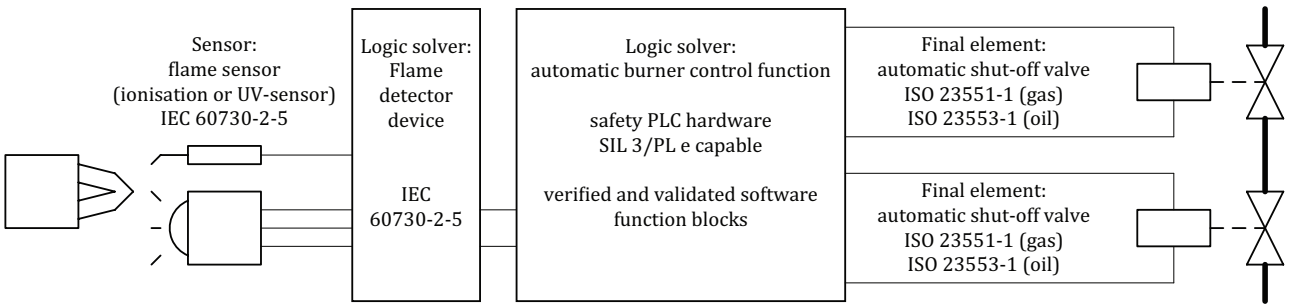
Figure E.3



NOTE 1 This figure shows one loop as an example for when applying 4.2.2 Method B.

NOTE 2 Safety function: high-temperature limit monitoring.

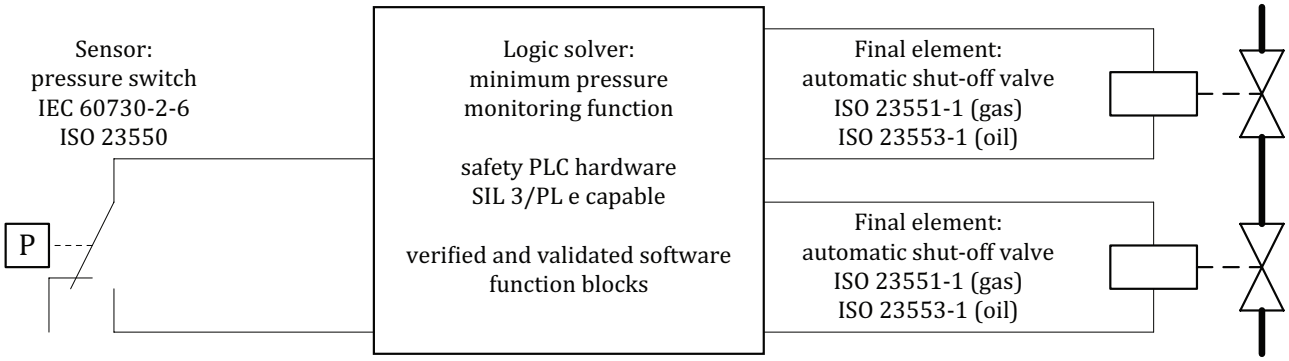
Figure E.4



NOTE 1 This figure shows one loop as an example for when applying 4.2.3 Method C.

NOTE 2 Safety function: flame monitoring.

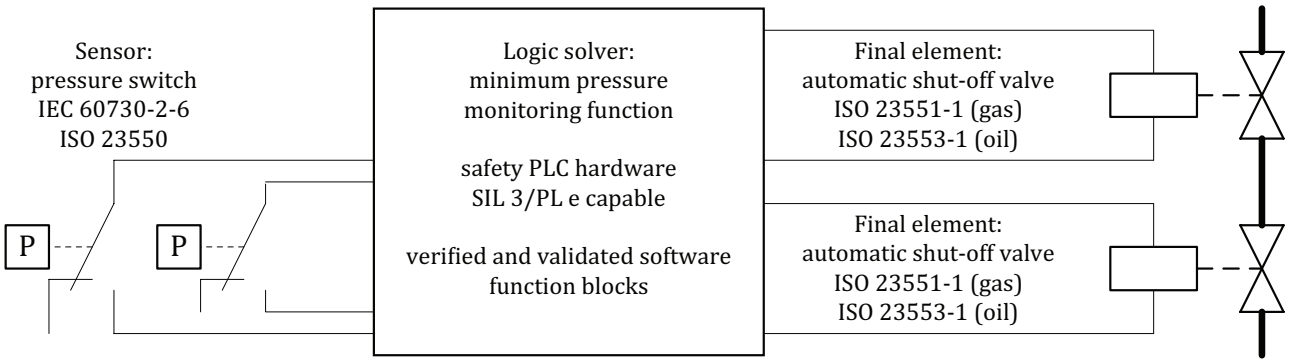
Figure E.5



NOTE 1 This figure shows one loop as an example for when applying 4.2.3 Method C.

NOTE 2 Safety function: minimum pressure monitoring.

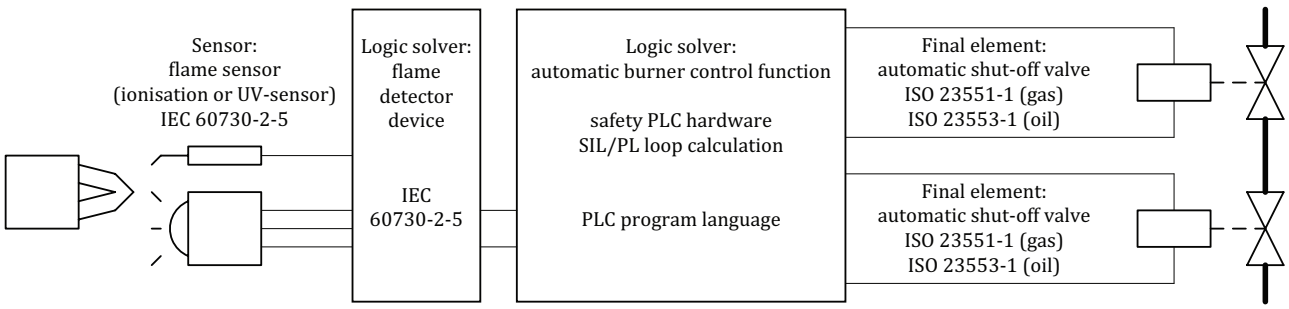
Figure E.6



NOTE 1 This figure shows one loop as an example for when applying 4.2.3 Method C.

NOTE 2 Safety function: minimum pressure monitoring.

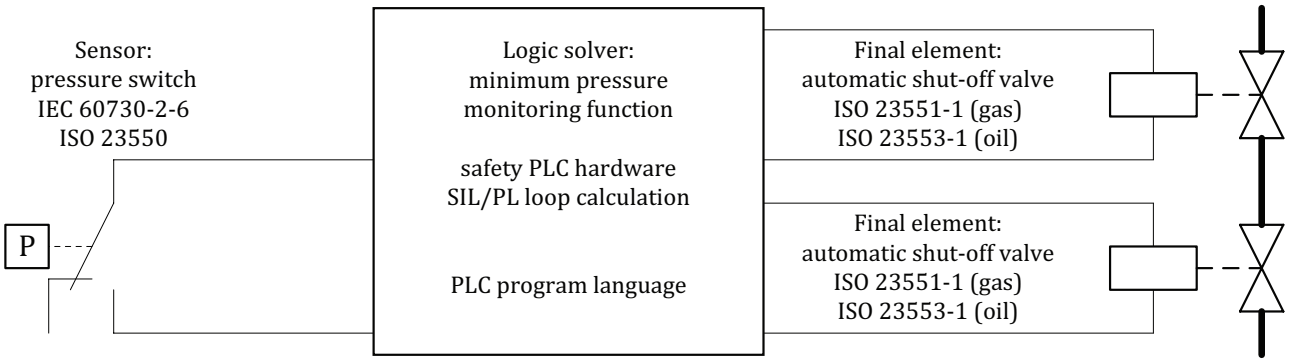
Figure E.7



NOTE 1 This figure shows one loop as an example for when applying 4.2.4 Method D.

NOTE 2 Safety function: flame monitoring.

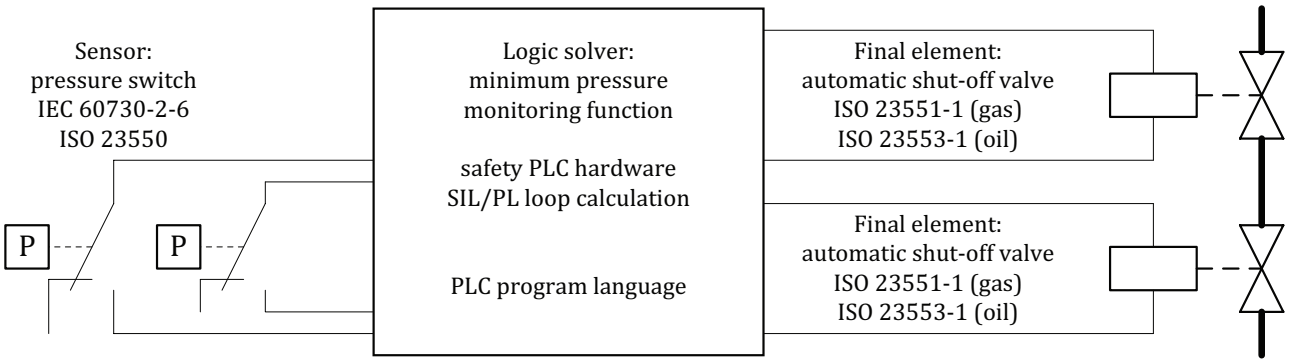
Figure E.8



NOTE 1 This figure shows one loop as an example for when applying 4.2.4 Method D.

NOTE 2 Safety function: minimum pressure monitoring.

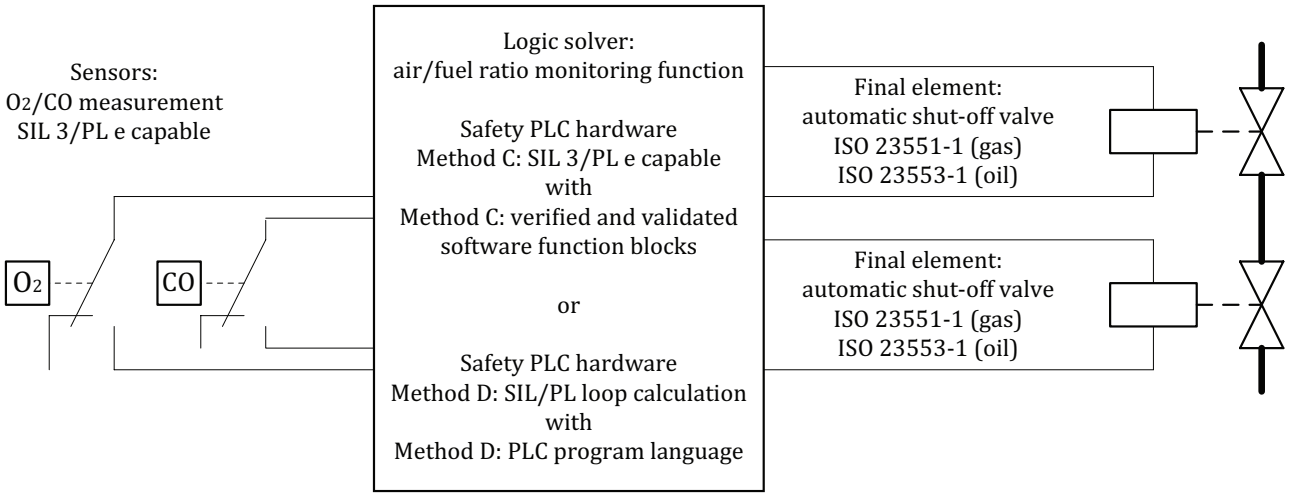
Figure E.9



NOTE 1 This figure shows one loop an example for when applying 4.2.4 Method D.

NOTE 2 Safety function: minimum pressure monitoring.

Figure E.10

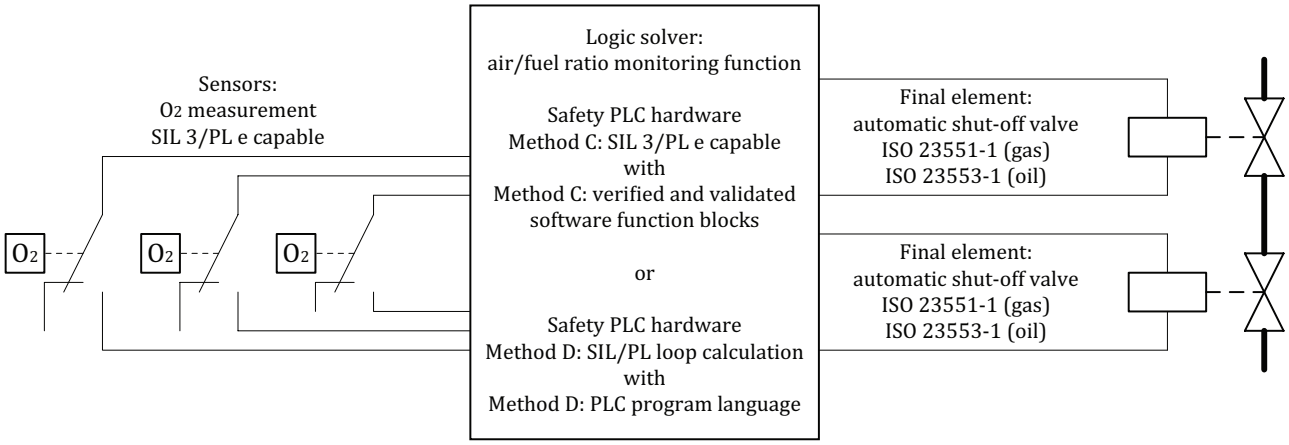


NOTE 1 This figure shows one loop an example for when applying 4.2.3 Method C or 4.2.4 Method D.

NOTE 2 Safety function: air/fuel ratio monitoring.

NOTE 3 The O_2/CO sensors and their sampling systems are selected with an appropriate response time.

Figure E.11

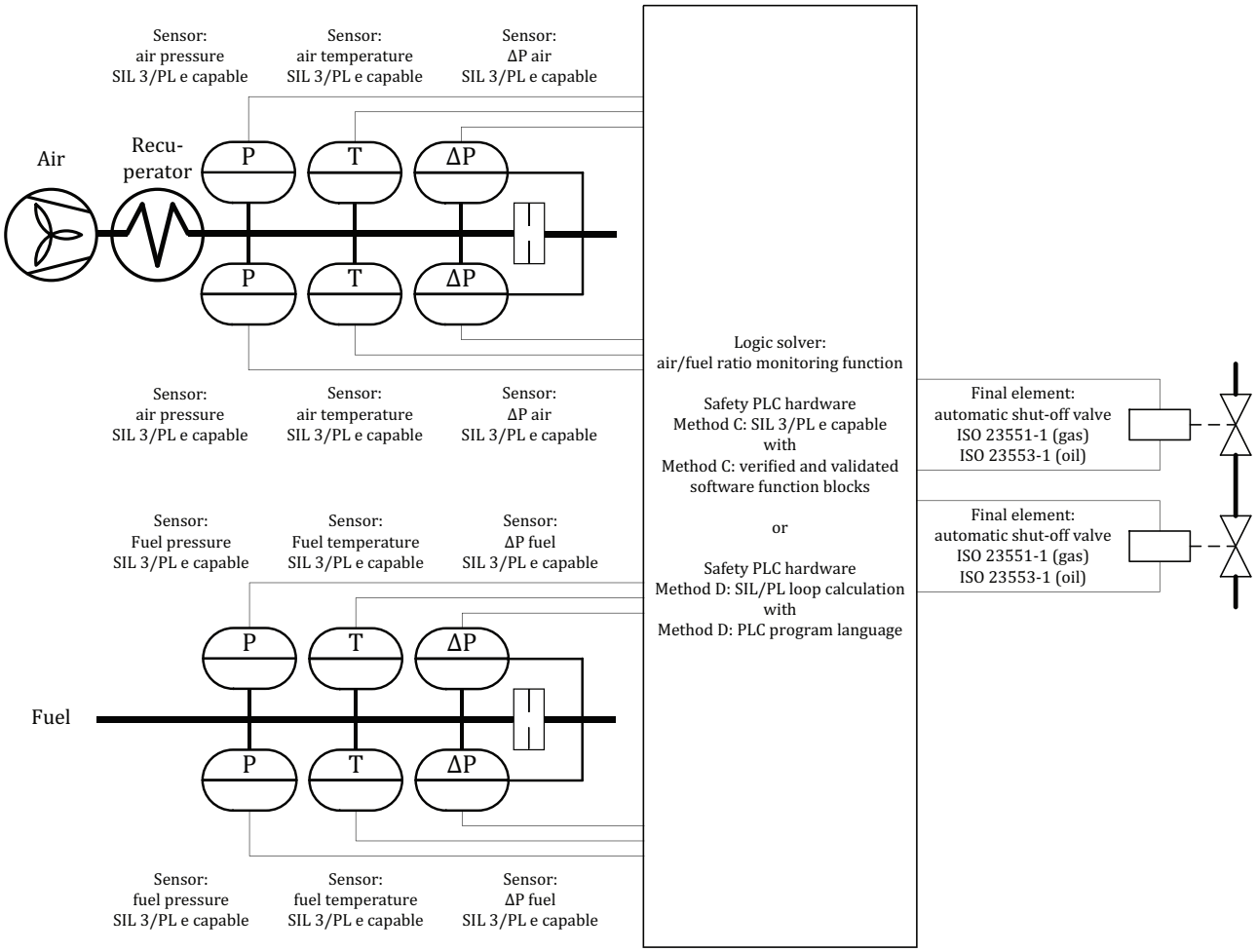


NOTE 1 This figure shows one loop an example for when applying 4.2.3 Method C or 4.2.4 Method D.

NOTE 2 Safety function: air/fuel ratio monitoring.

NOTE 3 The O_2 sensors and their sampling systems are selected with an appropriate response time.

Figure E.12



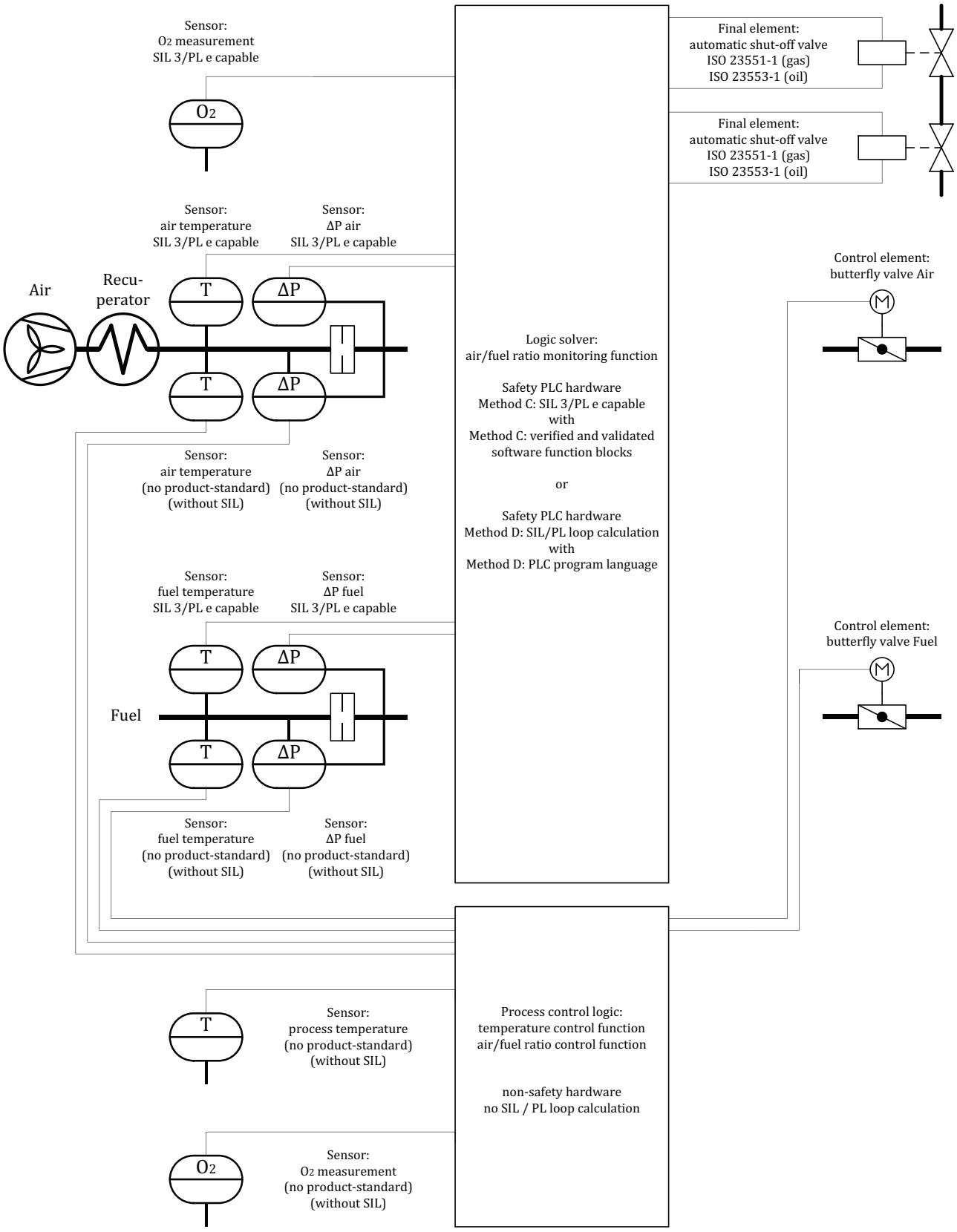
NOTE 1 This figure shows an example for when applying 4.2.3 Method C or 4.2.4 Method D.

NOTE 2 Safety function: Air/Fuel ratio monitoring.

NOTE 3 Additional measures are required in case of fuel with variable Wobbe index.

NOTE 4 See ISO 5167 (all parts) for calculation of flow rate.

Figure E.13

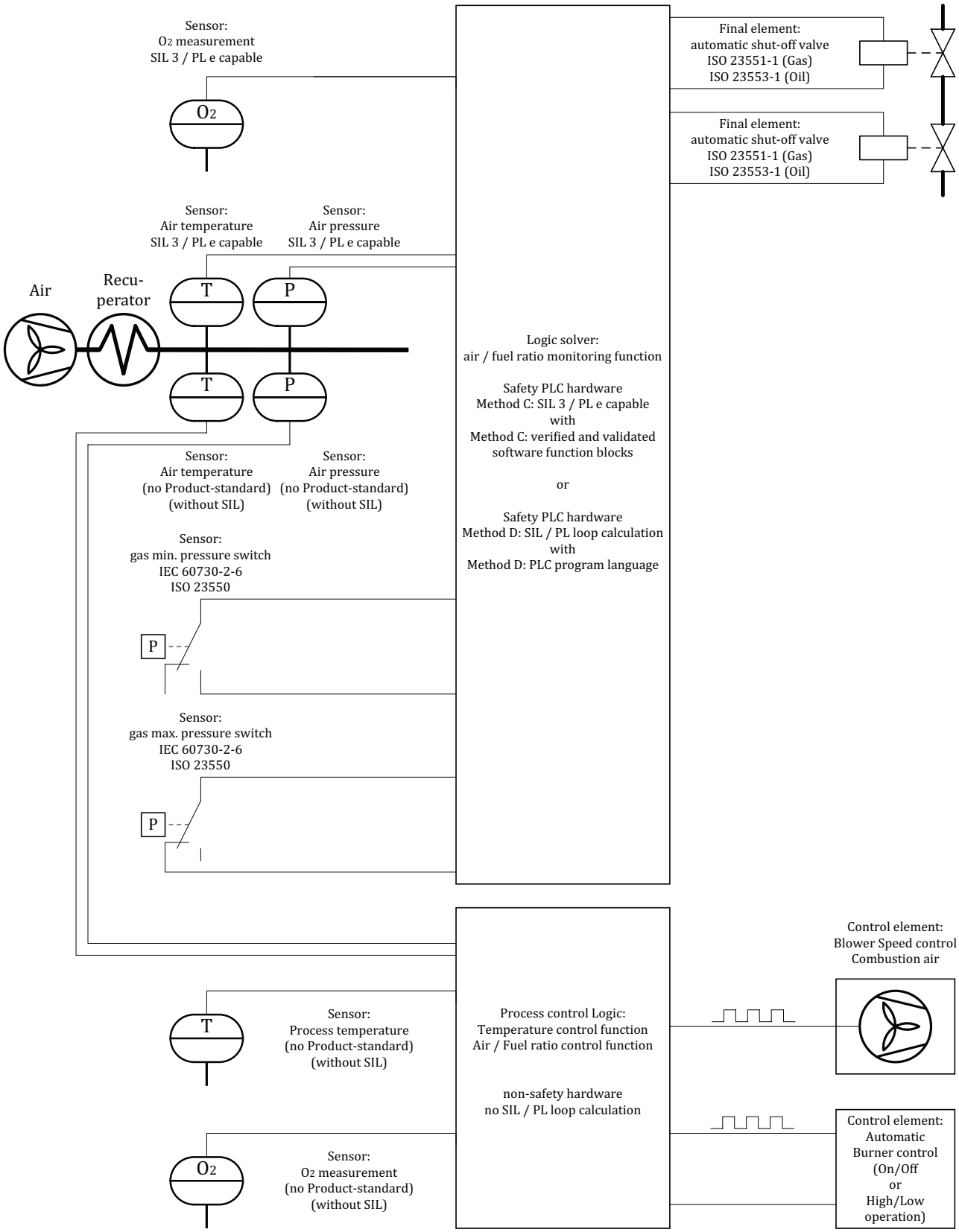


NOTE 1 This figure shows as an example of both a protective system and process control system for when applying 4.2.3 Method C or 4.2.4 Method D.

NOTE 2 Safety function: air/fuel ratio monitoring.

NOTE 3 The protective system O_2 sensor and sampling system is selected with an appropriate response time.

Figure E.14

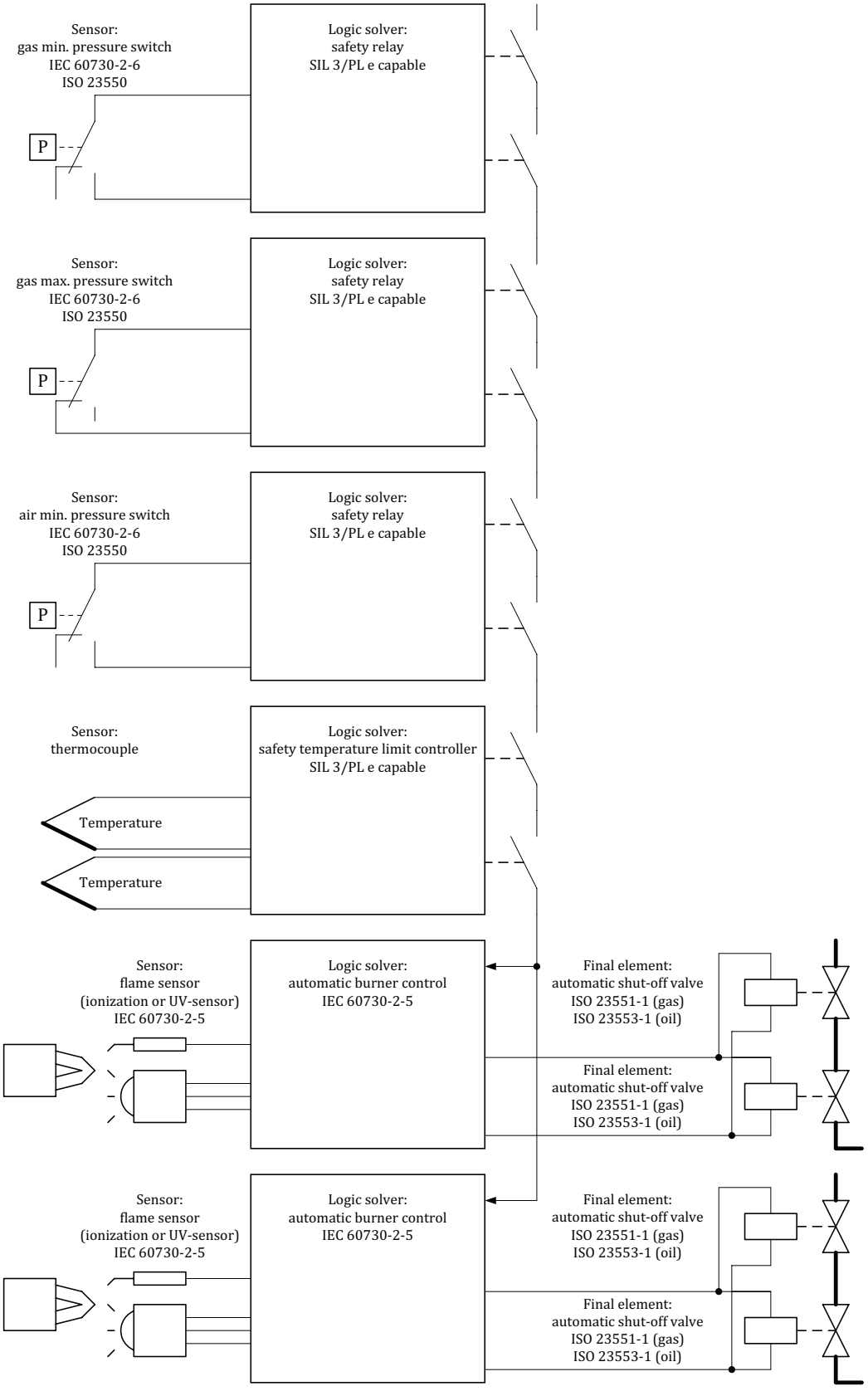


NOTE 1 This figure shows an example of both a protective system and process control system for when applying 4.2.3 Method C or 4.2.4 Method D.

NOTE 2 Safety function: air/fuel ratio monitoring.

NOTE 3 The protective system O_2 sensor and sampling system is selected with an appropriate response time.

Figure E.15



NOTE 1 This figure shows several loops as an example for when applying combined methods.

NOTE 2 Safety function: gas minimum pressure monitoring applying 4.2.2 Method B.

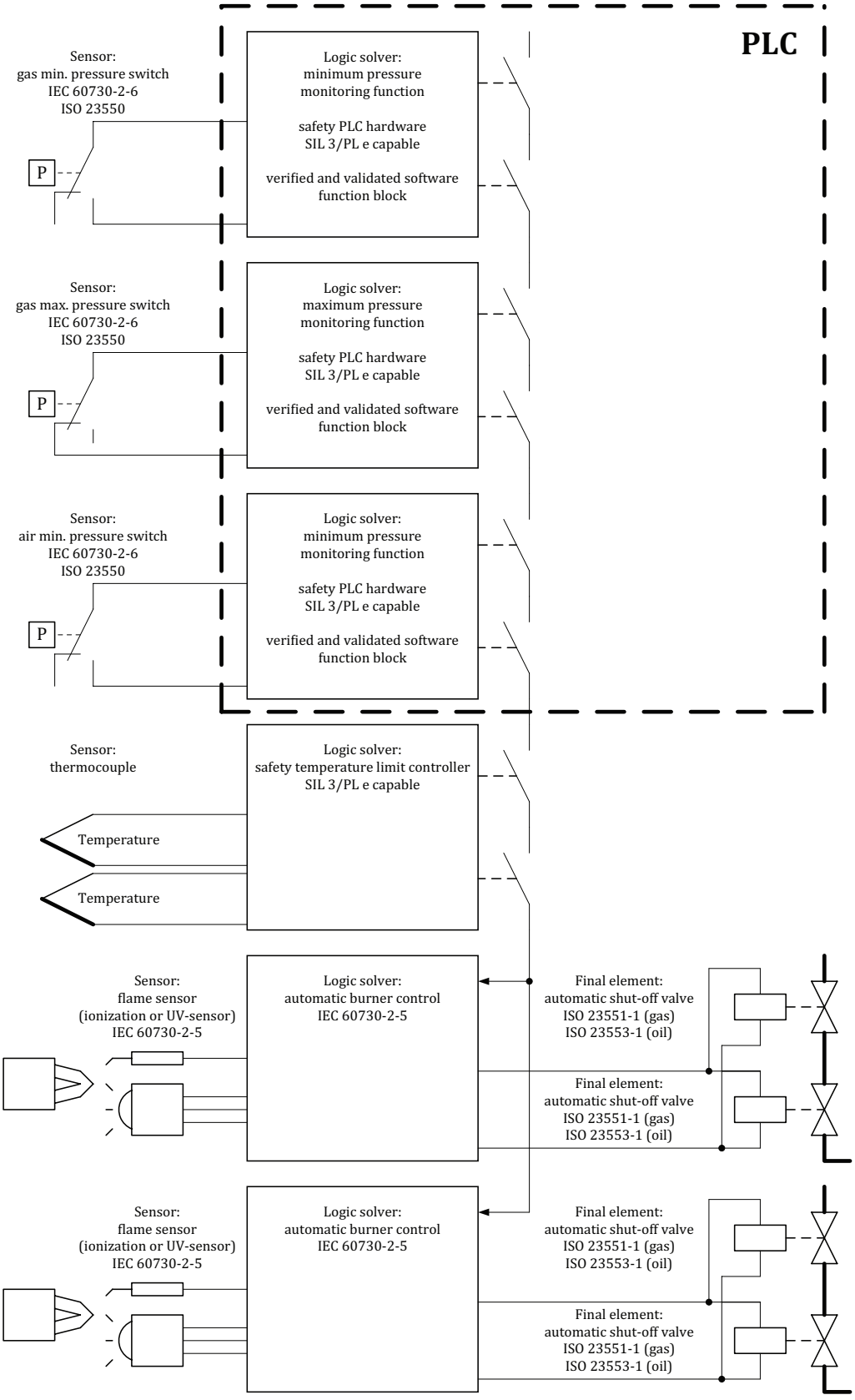
NOTE 3 Safety function: gas maximum pressure monitoring applying 4.2.2 Method B.

NOTE 4 Safety function: air minimum pressure monitoring applying 4.2.2 Method B.

NOTE 5 Safety function: high-temperature limit monitoring applying 4.2.2 Method B.

NOTE 6 Safety function: flame monitoring applying 4.2.1 Method A.

Figure E.16



NOTE 1 This figure shows several loops as an example for when applying combined methods.

NOTE 2 Safety function: gas minimum pressure monitoring applying 4.2.3 Method C.

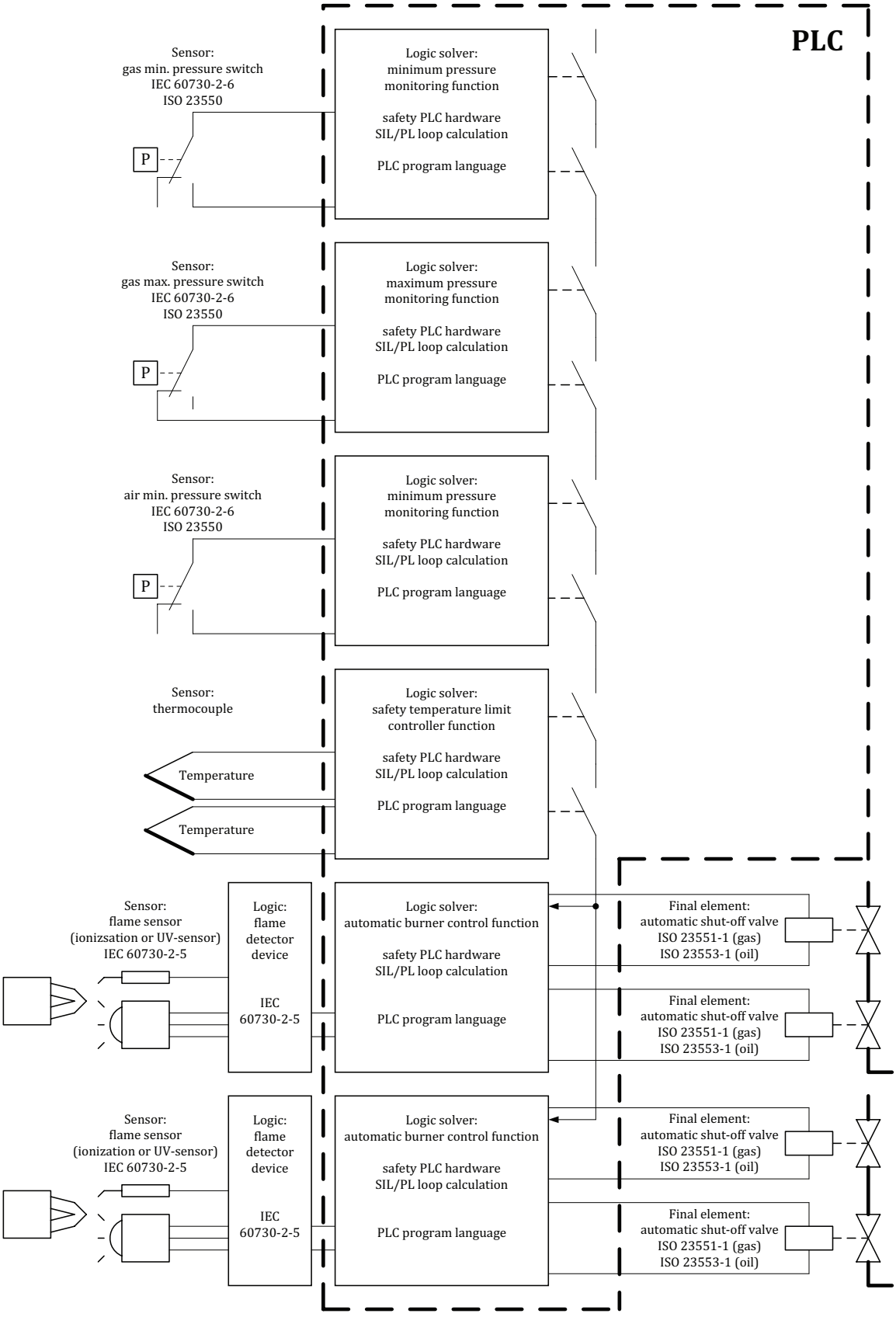
NOTE 3 Safety function: gas maximum pressure monitoring applying 4.2.3 Method C.

NOTE 4 Safety function: air minimum pressure monitoring applying 4.2.3 Method C.

NOTE 5 Safety function: high temperature limit monitoring applying 4.2.2 Method B.

NOTE 6 Safety function: flame monitoring applying 4.2.1 Method A.

Figure E.17



NOTE 1 This figure shows several loops as an example for when applying combined methods.

NOTE 2 Safety function: gas minimum pressure monitoring applying 4.2.4 Method D.

NOTE 3 Safety function: gas maximum pressure monitoring applying 4.2.4 Method D.

NOTE 4 Safety function: air minimum pressure monitoring applying 4.2.4 Method D.

NOTE 5 Safety function: high-temperature limit monitoring applying 4.2.4 Method D.

NOTE 6 Safety function: flame monitoring applying 4.2.4 Method D.

Figure E.18

Annex F
(normative)

Hardwiring protective systems

F.1 General

This annex describes how to hardwire the protective system so as not to reduce the level of safety. It also describes how to connect to the interlocks, final elements, etc.

This annex applies to the wiring within a hardwired logic solver and the wiring between the hardwired logic solver and the hardwired devices that directly or indirectly control the final elements.

This annex does not apply to the field wiring of the devices (interlocks, actuators, final elements, flame detector, igniter, etc.).

To maintain the level of safety of the hardwired 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 F.1 shall be applied for the design, fault analysis, and proof of safety.

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

F.2 Protection against faults of the logic solver

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 F.2 and F.3 or

   NOTE Examples of IMPROPER hardwiring are shown in Figures F.4, F.5, and F.6.

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 F.1. Any faults arising from a first fault (consecutive faults) shall be considered together with this first fault. See Figure F.7.

For systems for non-permanent (non-continuous) 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).

F.3 Measures to avoid faults

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

a) stipulation 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 rating of devices, and

c) functions and interconnections shall be verified by test.

Particular attention has to 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.

F.4 Hardware design

F.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.

F.4.2 Hardwired section of the protective system

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

Fault assessment for the protective system according to Figure F.1 shall consider failure of auxiliary power and break of connecting lines. 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 may be sufficient apart from the following measures.

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

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

For burners with permanent operation where regular inspections at sufficiently short intervals in accordance with Figure F.1 might not be performed, disconnecting devices (contactors, relays) with diverse functionality or hardware diversity shall be provided to shut down the entire fuel supply.

Reed relays shall not be used for any protective functions.

NOTE 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.

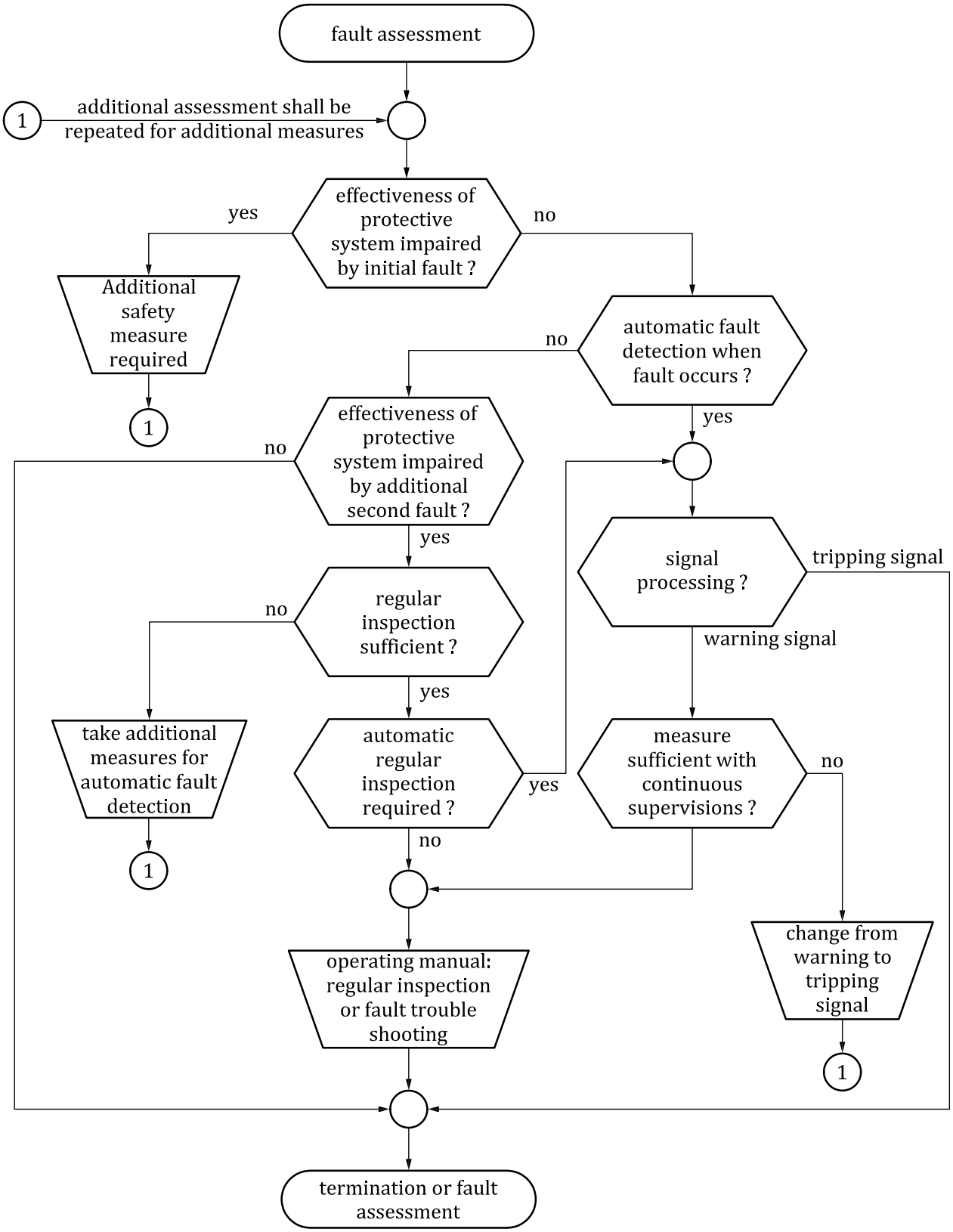
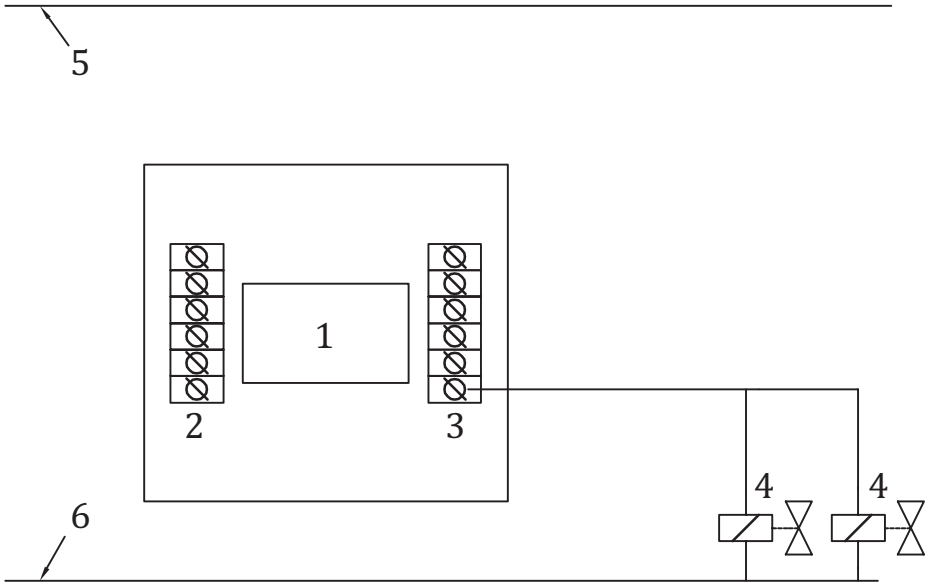


Figure F.1 — Fault assessment for the hardwired section of a protective system

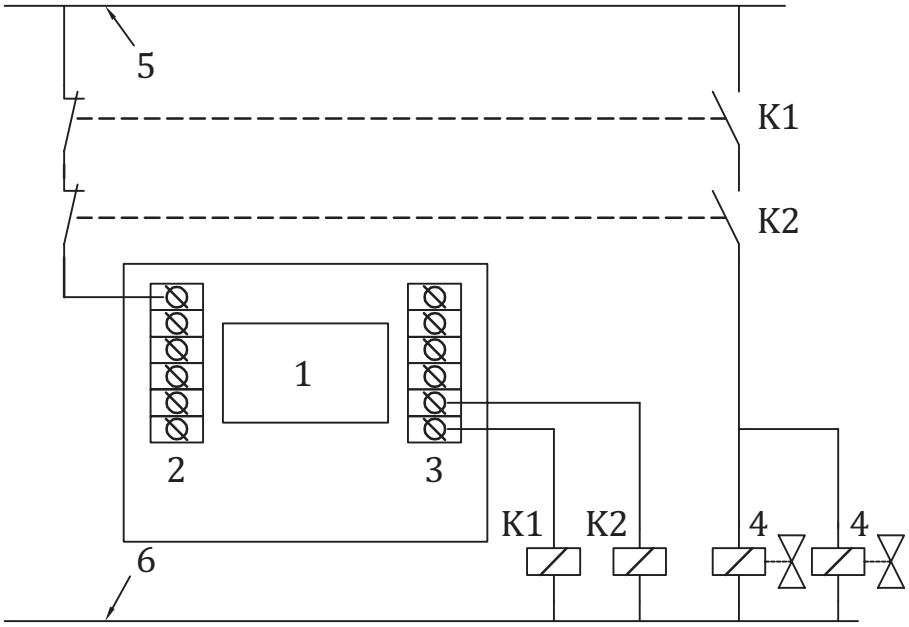


Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral

NOTE This figure shows safe output with redundancy and internal diagnosis.

Figure F.2 — Example of fault avoidance



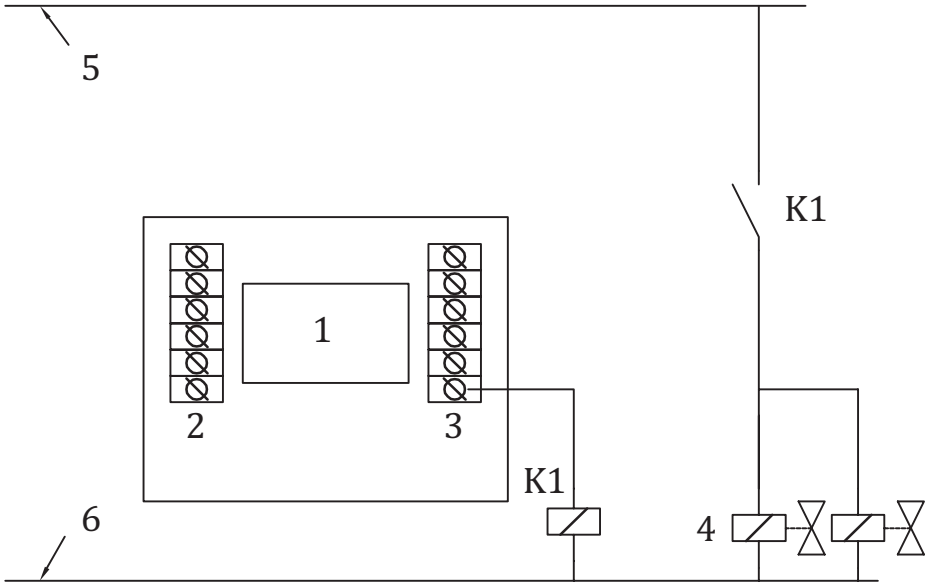
Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral
K1 relay 1
K2 relay 2

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

NOTE 2 For requirements for relays, see 4.3 a). See also Figure F.8 for basic configuration of relays used in safety circuits.

Figure F.3 — Example of fault avoidance



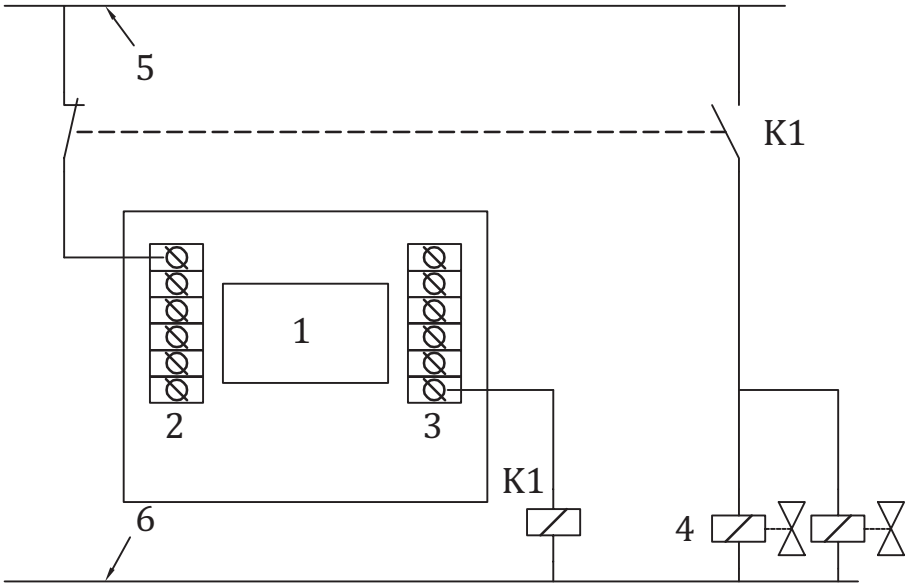
Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral
K1 relay 1

NOTE One single failure can be a hazardous failure. The failure is not detected.

Figure F.4 — Example of IMPROPER hardwiring

CAUTION — Figure F.4 shows an example of IMPROPER hardwiring even when relays as described in Figure F.8 are used.



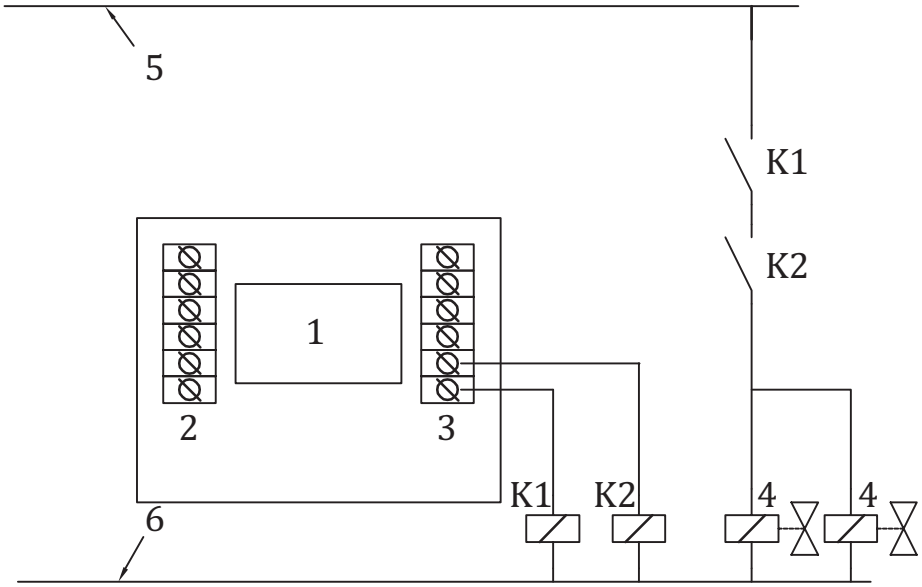
Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral
K1 relay 1

NOTE Relay failure is detected. One single relay failure can be hazardous.

Figure F.5 — Example of IMPROPER hardwiring

CAUTION — Figure F.5 shows an example of IMPROPER hardwiring even when relays as described in Figure F.8 are used.



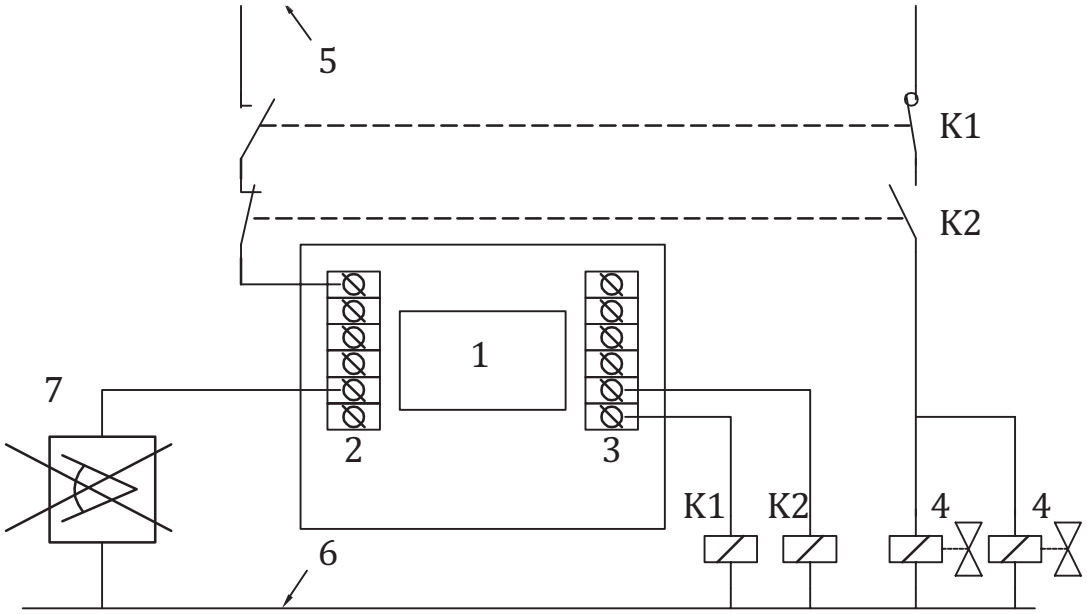
Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral
K1 relay 1
K2 relay 2

NOTE One single failure avoids hazard, but since relay failures are undetected, failures can accumulate and result in a hazard.

Figure F.6 — Example of IMPROPER hardwiring

CAUTION — Figure F.6 shows an example of IMPROPER hardwiring even when relays as described in Figure F.8 are used.



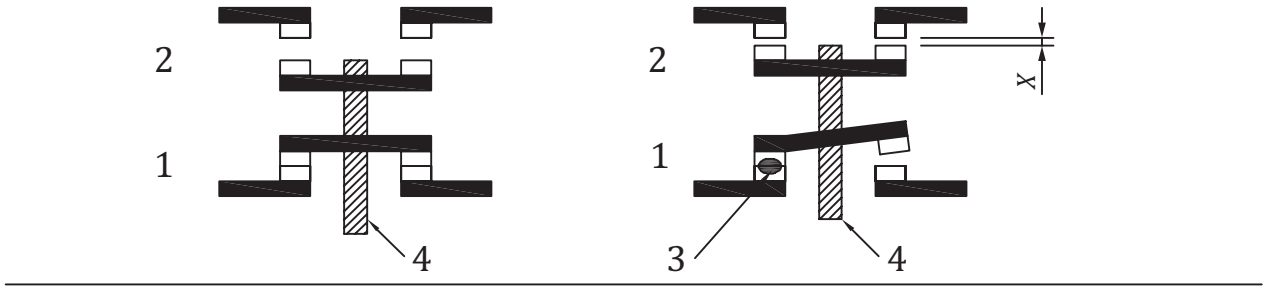
Key

1 logic solver(s)
2 safe input
3 safe output
4 fuel valves
5 valve voltage
6 neutral
7 flame sensor
K1 relay 1 (fault)
K2 relay 2

One failure in relay 1 is detected as a first fault. Logic closes fuel valves. Flame failure is a consecutive fault which shall not be taken into account as primary fault.

NOTE For requirement for relays, see 4.3 a). See also Figure F.8 for explanation of relays with forced guided contacts.

Figure F.7 — Example of a consecutive fault



Key

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

Relays used in safety circuits with feedback of the relay position shall be with forced guided 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 F.8 — Example of relay with forced guided contacts

Bibliography

[1] ISO 5167 (all parts), *Measurement of fluid flow by means of orifice plates, nozzles and Venturi tubes inserted in circular cross-section conduits running full*

[2] ISO 14118, *Safety of machinery — Prevention of unexpected start-up*

[3] ISO 13850, *Safety of machinery — Emergency stop function — Principles for design*

[4] ISO 23550, *Safety and control devices for gas burners and gas-burning appliances — General requirements*

[5] ISO 23551-1:2012, *Safety and control devices for gas burners and gas-burning appliances — Particular requirements — Part 1: Automatic and semi-automatic valves*

[6] ISO 23551-4:2005, *Safety and control devices for gas burners and gas-burning appliances — Particular requirements — Part 4: Valve-proving systems for automatic shut-off valves*

[7] ISO 23553-1:2007, *Safety and control devices for oil burners and oil-burning appliances — Particular requirements — Part 1: Shut-off devices for oil burners*

[8] IEC 60730-2-6:2007, *Automatic electrical controls for household and similar use — Part 2-6: Particular requirements for automatic electrical pressure sensing controls including mechanical requirements*

[9] IEC 61511-3:—*Functional safety - Safety instrumented systems for the process industry sector*

[10] ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*

[11] EN 14597, *Temperature control devices and temperature limiters for heat generating systems*

ICS 13.100;25.180.01
Price based on 71 pages

This page deliberately left blank

British Standards Institution (BSI)

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

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

About us

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

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

Information on standards

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

Buying standards

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

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

Subscriptions

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

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

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

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

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

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

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

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

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

Copyright

Useful Contacts:

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

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

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

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

bsi.

...making excellence a habit.™