INTERNATIONAL STANDARD

ISO 13577-4

Second edition
2022-07

Industrial furnaces and associated processing equipment — Safety —

Part 4: Protective systems

Fours industriels et équipements associés — Sécurité —

Partie 4: Systèmes de protection

Reference number
ISO 13577-4:2022(E)

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

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Design requirements for equipment in a protective system ... **4**
4.1 General ... 4
4.2 Requirements for protective systems ... 6
4.2.1 Overview of methods ... 6
4.2.2 Method A ... 7
4.2.3 Method BC ... 8
4.2.4 Method D ... 10
4.3 Fault assessment for the wired section of protective systems ... 11
4.4 Failure of utilities ... 12
4.5 Reset ... 12
5 Information for use ... **12**
Annex A (informative) **Explanation of techniques and measures for avoiding systematic faults** ... **13**
Annex B (normative) **Wiring of protective systems** ... **15**
Annex C (informative) **Examples for the determination of safety integrity level (SIL) or performance level (PL) using the risk graph method** ... **29**
Annex D (informative) **Example of a risk assessment for one safety instrumented function using the method according to the IEC 61511:2016 series** ... **45**
Annex E (informative) **Examples for protective functions** ... **53**
Annex F (normative) **Requirements for application software** ... **82**
Bibliography ... **84**

Foreword

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

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

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

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

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

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

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

The main changes are as follows:

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

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

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

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

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

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

Introduction

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

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

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

Industrial furnaces and associated processing equipment — Safety —

Part 4: Protective systems

1 Scope

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[SOURCE: ISO 13574:2015, 2.164]

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

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

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

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

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

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

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

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

4 Design requirements for equipment in a protective system

4.1 General

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

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

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

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

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

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

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

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

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

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

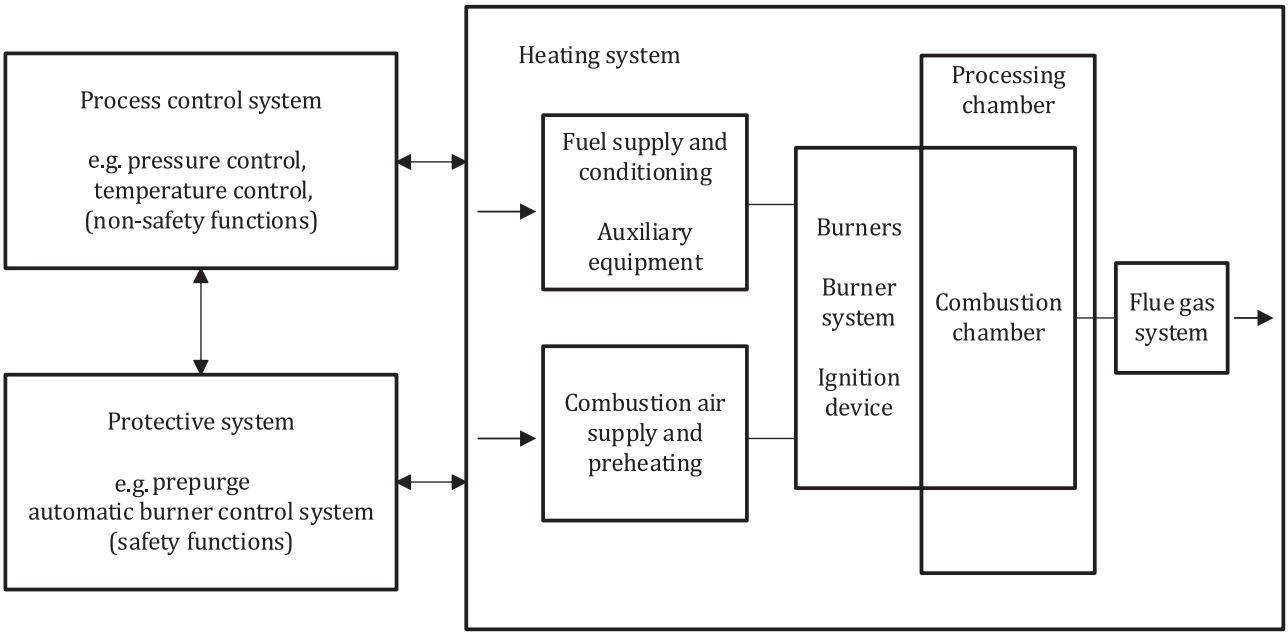

Figure 1 — Block diagram of control and protective systems

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

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

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

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

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

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

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

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

4.2 Requirements for protective systems

4.2.1 Overview of methods

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

— method A as specified in 4.2.2;

— method BC as specified in 4.2.3;

— method D as specified in 4.2.4.

Figure 2 shows the basic configuration of a protective system.

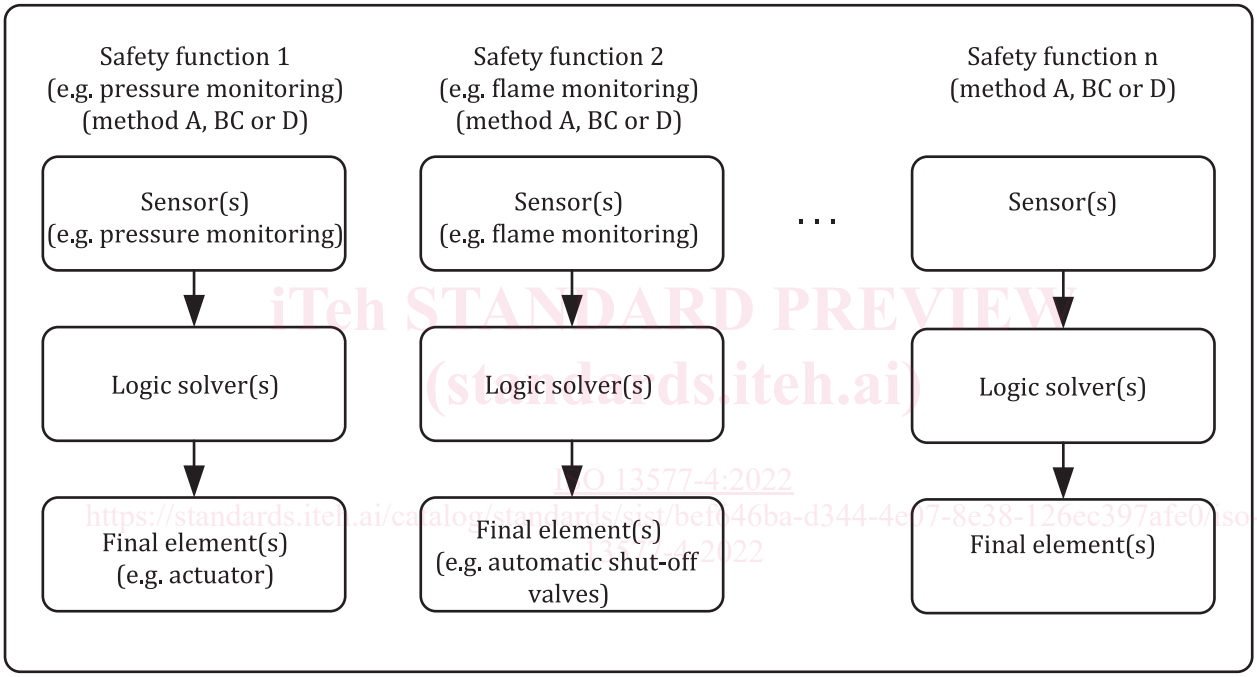

Figure 2 — Basic configuration of a protective system

Figure 3 shows the basic characteristics of each method.

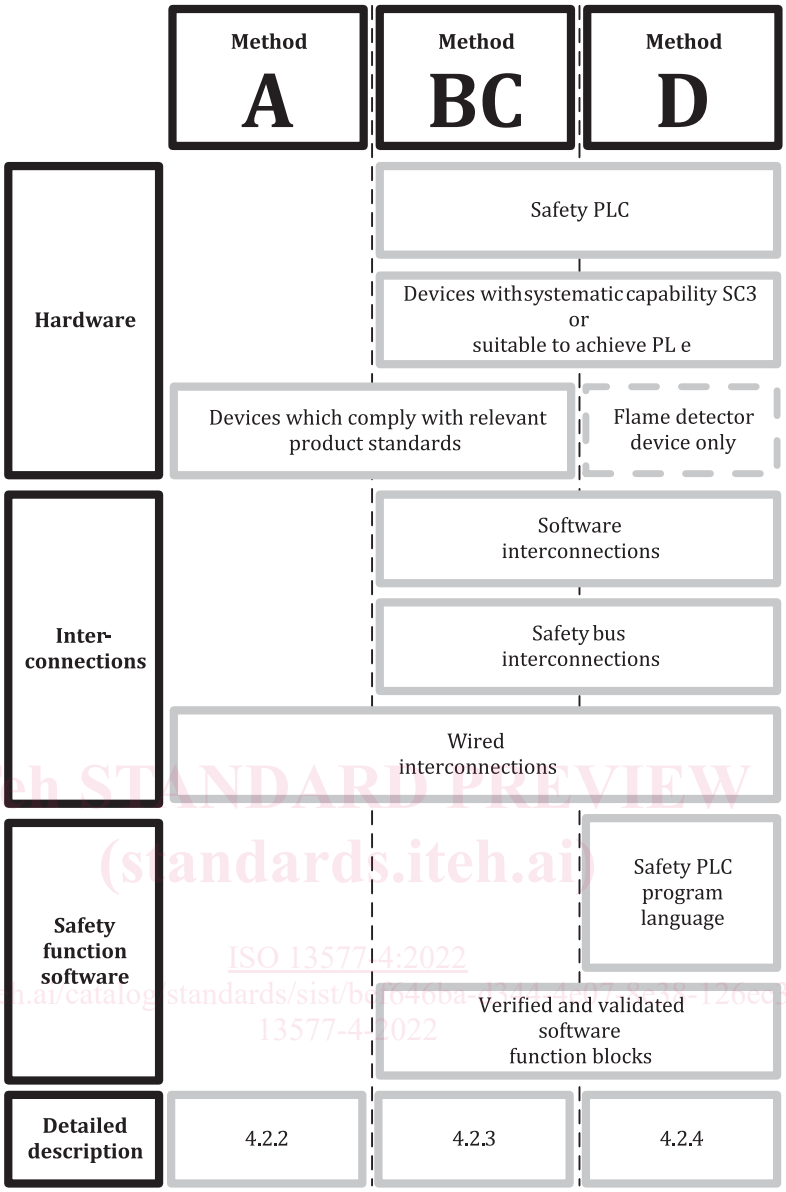

Figure 3 — Method overview

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

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

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

4.2.2 Method A

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

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

The following requirements for wiring shall be fulfilled:

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

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

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

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

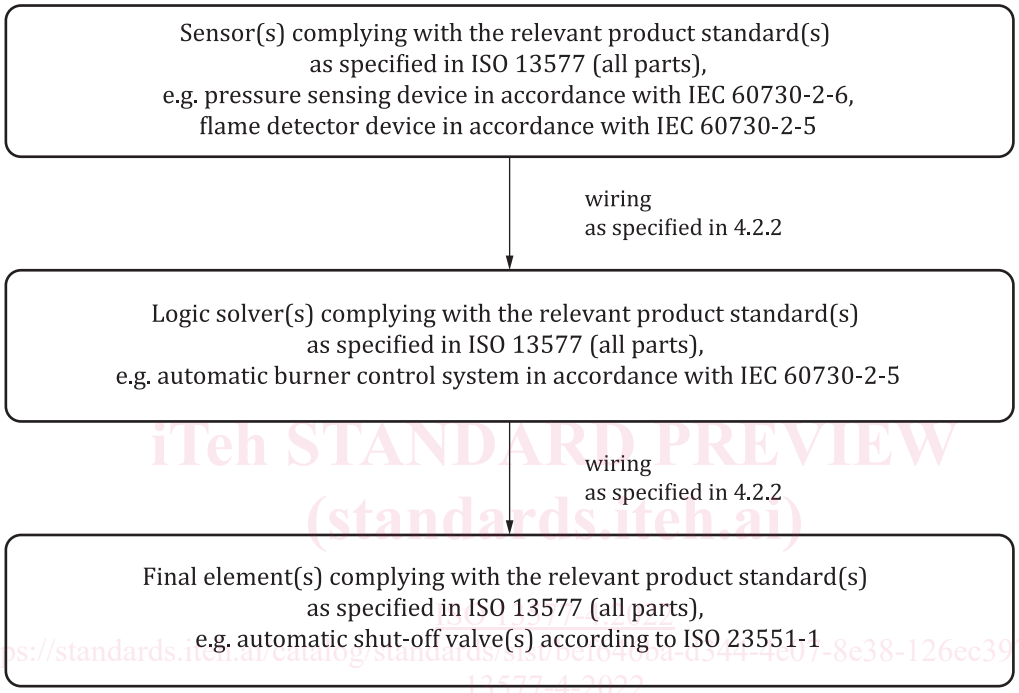

Figure 4 — Hardware configuration of Method A

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

4.2.3 Method BC

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

The following requirements for wiring shall be fulfilled:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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