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.

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.

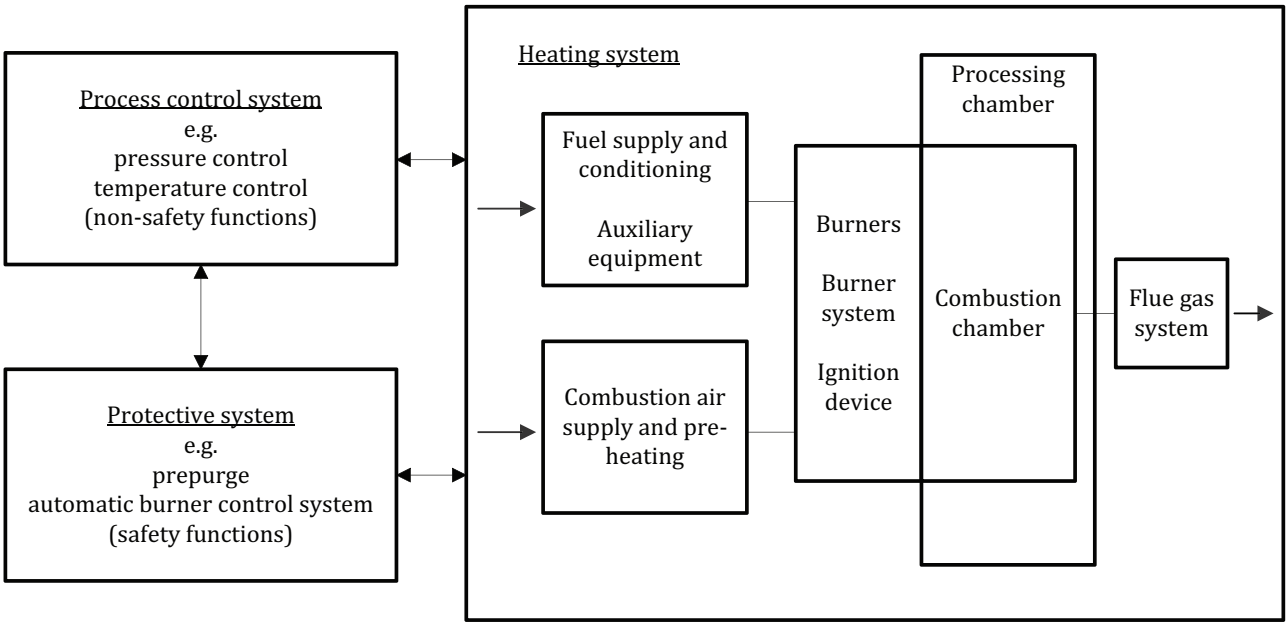

Figure 1 — Block diagram of control and protective systems

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.

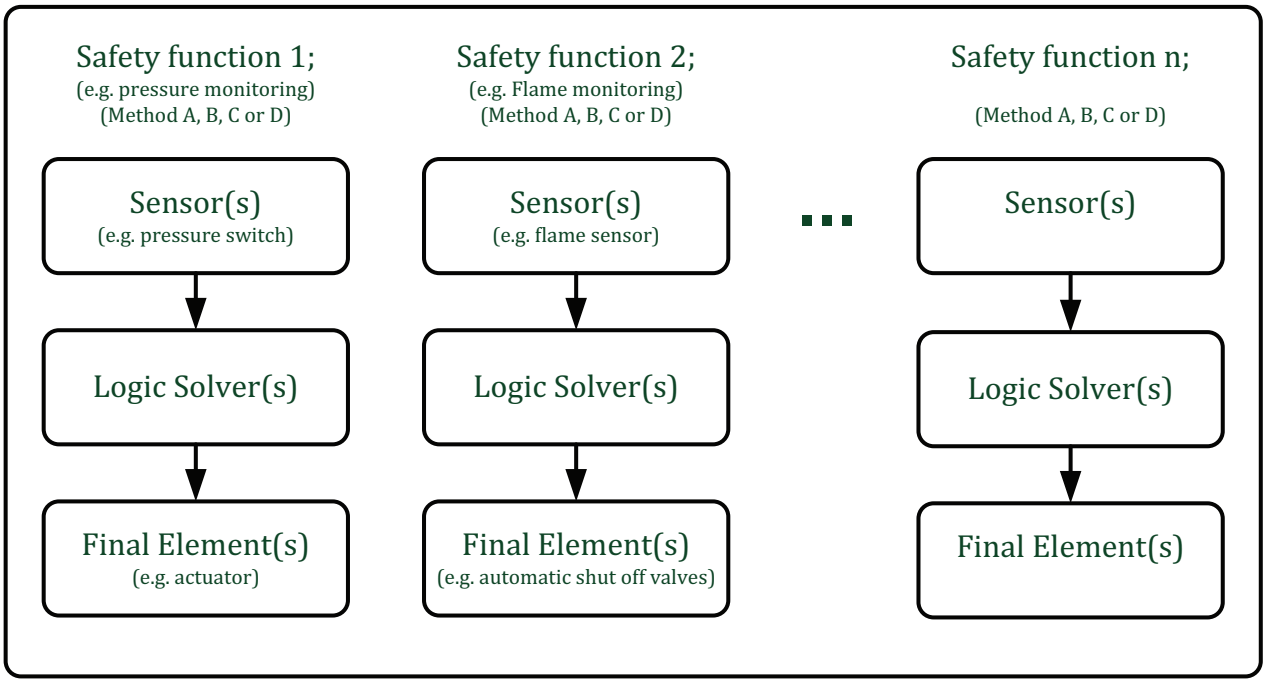

Figure 2 — Basic configuration of a protective system

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).

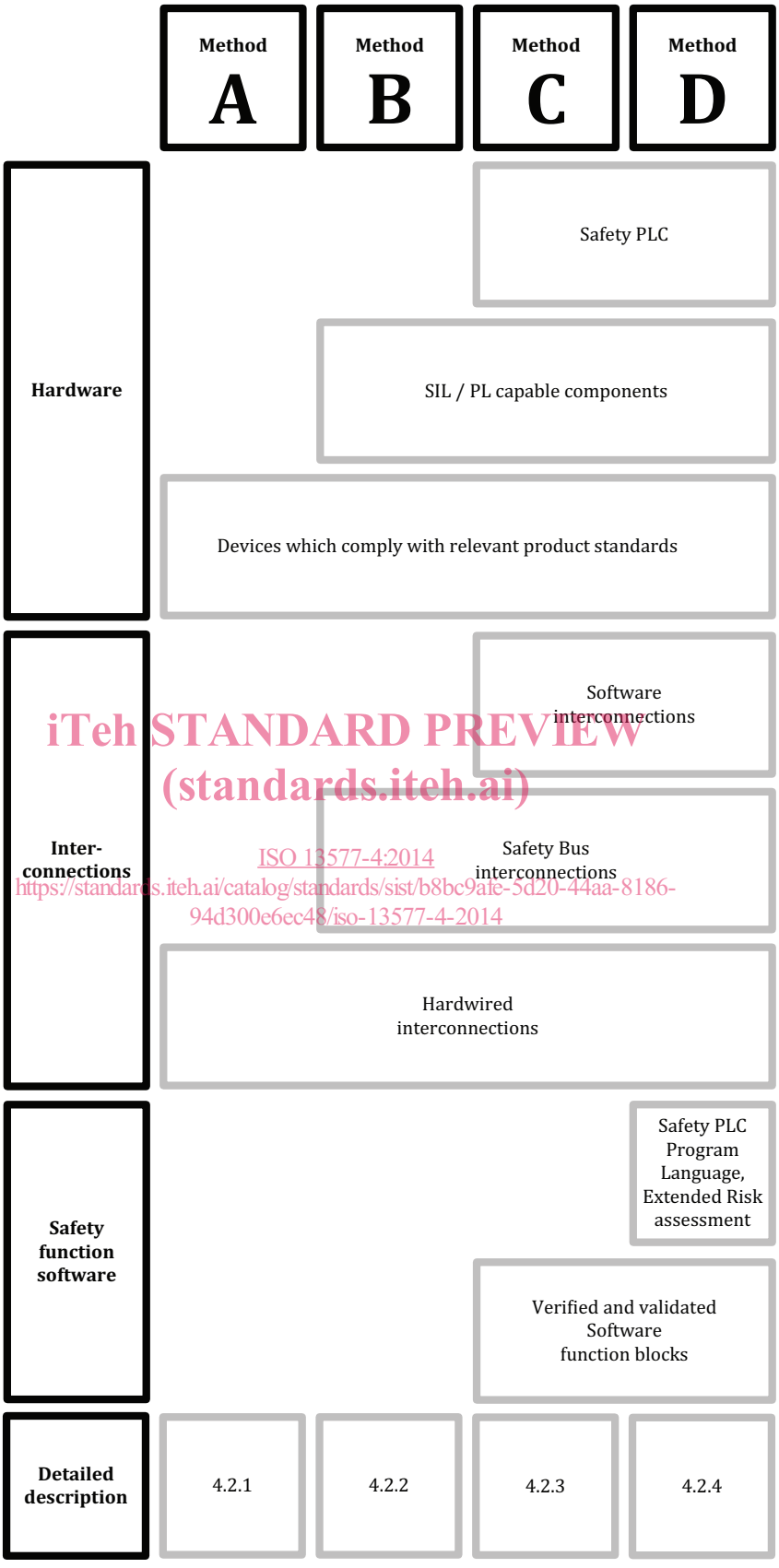

Figure 3 — Method overview

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.

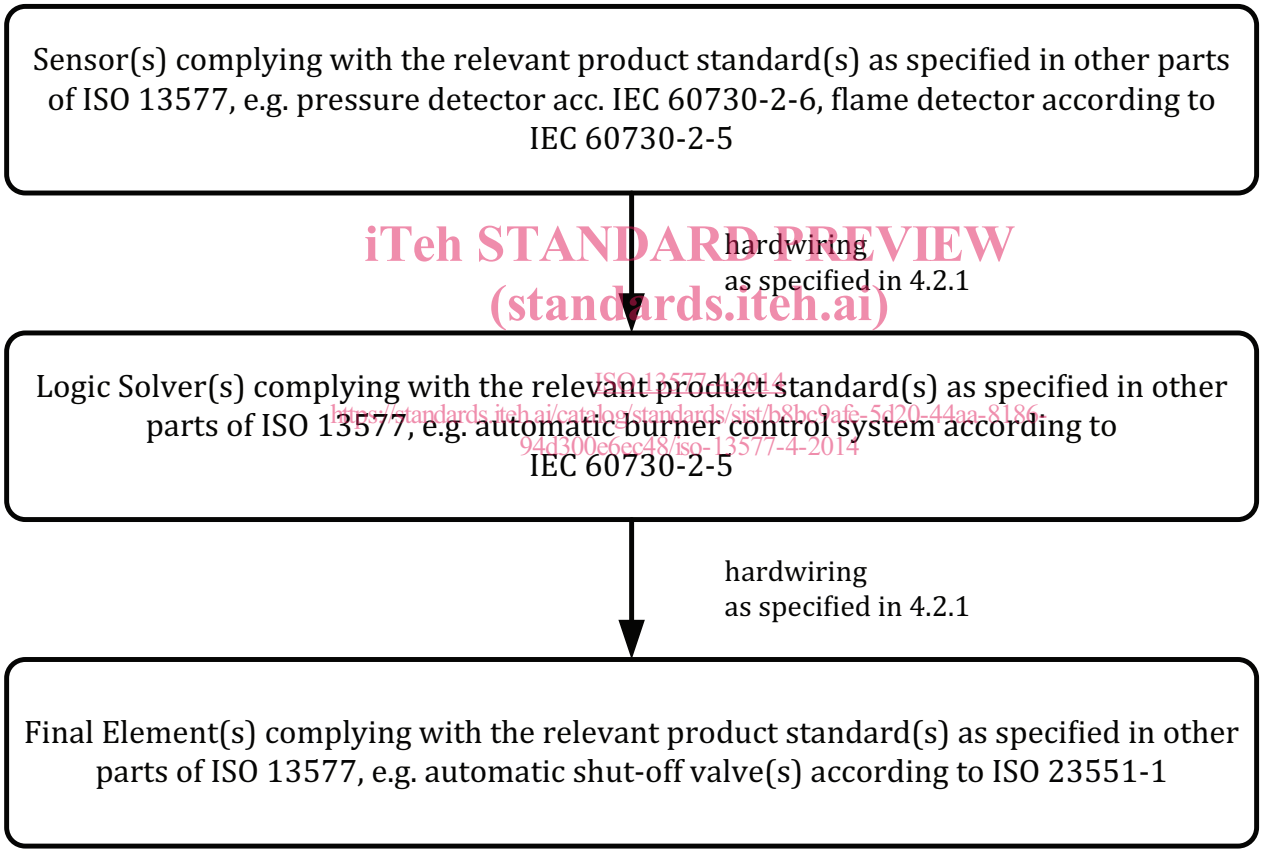

Figure 4 — Hardware configuration of Method A

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.