DRAFT INTERNATIONAL STANDARD ISO/DIS 13577-4

ISO/TC **244** Secretariat: **JISC**

Voting begins on **2013-05-27** Voting terminates on **2013-08-27**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Industrial furnace and associated processing equipement — Safety —

Part 4: Protective systems

Fours industriels et équipements associés — Sécurité —

Partie 4: Systèmes de protection

ICS 13.180; 25.180.01

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

COPYRIGHT PROTECTED DOCUMENT

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 v

Introduction vi

1. Scope 7

2. Normative references 7

3. Terms and definitions 7

4. Design requirements for equipment in a Protective System. 10
4.1 General 10
4.2 Requirements for protective systems 11
4.2.1. Method A 13
4.2.2. Method B 13
4.2.3. Method C 15
Method D 18
4.2.4. 18
4.3 Fault assessment for the hardwired section of protective systems 19
4.4 Failure of utilities 20
4.5 Reset 20

Annex A (informative) **Explanation of techniques and measures for avoiding systematic faults** 21
A.1 General 21
A.2 Competency 21
A.3 Avoidance of systematic faults 21

Annex B (informative) **Examples of techniques for avoiding failures from external wiring** 23

Annex C (informative) **Examples for the determination of safety integrity level SIL using the risk graph method** 27
C.1 General 27
C.2 Examples for the determination of the required SIL/PL 28
C.2.1 Example 1 – Table C.1 28
C.2.2 Example 2 – Table C.2 28
C.2.3 Example 3 – Table C.3 28
C.2.4 Example 4 – Table C.4 28
C.2.5 User's guide for risk graph according IEC 61511 (i.e. Table C.3 and C.4) 43

Annex D (informative) **Example of an extended risk assessment for one safety instrumented function using IEC 61511 method** 47
D.1 General 47
D.2 Concept description of equipment under control 47
D.3 Hazard and risk assessment 47
D.3.1 Initiating events 47
D.3.2 Hazard – process deviation – insufficient combustion air 48
D.4 Consequences 48
D.5 Event tree example 49
D.6 Safety System Functional Requirements 49
D.6.1 Safe State 50
D.6.2 Demand Rate 50
D.6.3 Spurious Trip Rate 50
D.6.4 Proof Test Interval 50
D.6.5 Process Safety Time 50
D.6.6 System Response Time 50
D.7 Safety Sensor Functional Requirements 50
D.8 Logic Solver Requirements Including Alarming, External Comparision and HMI ... 52
D.9 Final Element Requirements 52

D.10 Manual Intervention Requirements **53**
D.11 Startup Requirements **53**

Annex E (informative) Example schematics of protective system **55**

Annex F (normative) **Hardwiring protective systems for methods A, B and C** **62**
F.1 General **62**
F.2 Protection against faults of the logic solver/box **62**
F.3 Measures to avoid faults **63**
F.4 Hardware design **63**
F.4.1 General requirements of the hardware **63**
F.4.2 Hard-wired section of the protective system **63**

Bibliography **72**

The **table of contents** is an optional preliminary element, but is necessary if it makes the document easier to consult. The table of contents shall be entitled “Contents” and shall list clauses and, if appropriate, subclauses with titles, annexes together with their status in parentheses, the bibliography, indexes, figures and tables. The order shall be as follows: clauses and subclauses with titles; annexes (including clauses and subclauses with titles if appropriate); the bibliography; indexes; figures; tables. All the elements listed shall be cited with their full titles. Terms in the “Terms and definitions” clause shall not be listed in the table of contents.

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 13577-4 was prepared by Technical Committee ISO/TC 244, *Industrial furnaces and associated processing equipment*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

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

— *Part 4: Protective systems*

— Part 1: General requirements

— Part 2: Requirements for combustion and fuel handling systems

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

Introduction

This document was developed to specify the requirement 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 the other parts of ISO 13577.

This part of ISO 13577 provides 4 methods which manufacturers of TPE are to choose in designing the protective system of TPE.

This document is part of a Type C standard as defined in ISO 12100. 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 is more suitable for the design of a TPE protective system.

IEC 61511 provides the option of 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 may be chosen as an alternative. .

Industrial furnaces 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 referenced documents are indispensable for the application 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 thermal processing equipment —Vocabulary*

ISO 13577-1, *Industrial furnaces and associated thermal processing equipment — Safety – Part 1: General requirements*

ISO 13577-2, *Industrial furnaces and associated thermal processing equipment — Safety – Part 2: Combustion and fuel handling systems*

ISO 13577-3, *Industrial furnaces and associated thermal processing equipment — Safety – Part 3: Generation and use of protective and reactive atmosphere gases*

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

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), *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 and the following apply.

3.1
final element
The device(s) controlled by the logic solver to affect the process being monitored by the sensor. In a protective system, it is the part that physically acts (e.g. actuator, automatic shutoff valve, relay, etc…) to bring the safety function to a safe state.

3.2
flame detector device
device by which the presence of a flame is detected and signaled; it can consist of a flame sensor, an amplifier and a relay for signal transmission

NOTE This term and definition is given in ISO 13574

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

NOTE This term and definition is given in ISO 13574

3.4
logic function
function which 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); logic functions are executed by the logic solver of a protective system.

[SOURCE: IEC 61511-1:2003 3.2.39 modified]

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

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

[SOURCE: IEC 61511-1:2003 3.2.40 modified]

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

NOTE This term and definition is given in ISO 13574

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
the standards for products and devices which are listed in the other parts of ISO 13577

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

NOTE This term and definition is given in ISO 13574

3.10
protective system
instrumented system used to implement one or more safety related instrumented functions. A protective system is composed of any combination of sensor(s), logic solver(s), and final elements. (For example see figure 2).

NOTE This can include either safety related instrumented control functions or safety related instrumented protection functions or both.

[SOURCE: IEC 61511-1:2003, 3.2.72 modified]

3.11
safety bus
A bus system and / or protocol for digital network communication between safety devicedevices that is designed to achieve and / or maintain a safe state of the protective system in compliance with IEC 61508 or IEC 60730-2-5.

3.12
safety device
A device which is used to perform protective functions, either on its own or as a part of a protective system (e.g. sensors, limiters, flame monitors, burner control systems, logic systems, final elements, automatic shut-off valves etc.)

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 the target failure measures for the four safety integrity levels are specified in Table 2 and 3 of IEC 61508-1.

NOTE 2 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 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
Limiter, transducer or any other monitoring device which outputs a signal and/or cuts out and only reverses the output signal in the event of a specific change in the performance quantity (e.g. pressure, temperature, flow, level).

3.15
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 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 What is a relevant systematic failure mechanism will depend 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 will be necessary to consider both systematic hardware and software failure mechanisms.

NOTE 3 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: IEC 61508-4:2010 3.5.9]

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.

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.

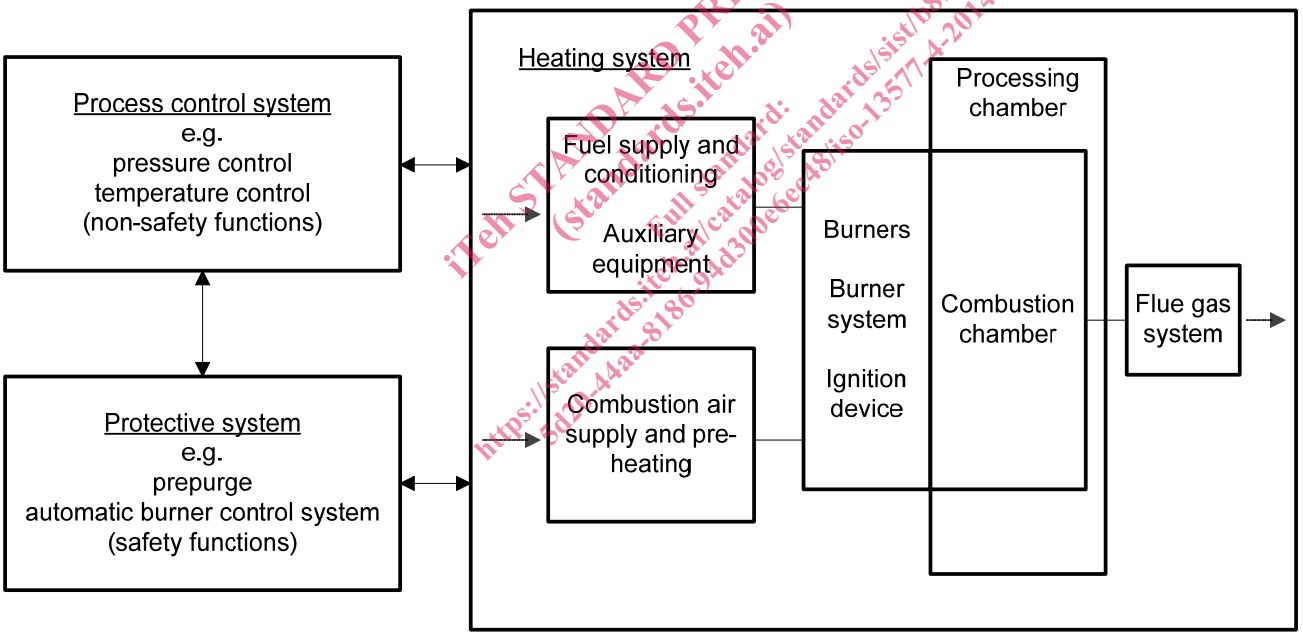

Figure 1 — Block diagram of control and protective systems

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 Informative Annex A.

Failure due to short circuit in external wiring shall be avoided. See Informative 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 year.

See informative 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 below shall be used to implement a protective system for the safety function(s) requirements identified in other parts of 13577, however, only one method shall be used for any one specific safety function:

— 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 is showing the basic configuration of a protective system.

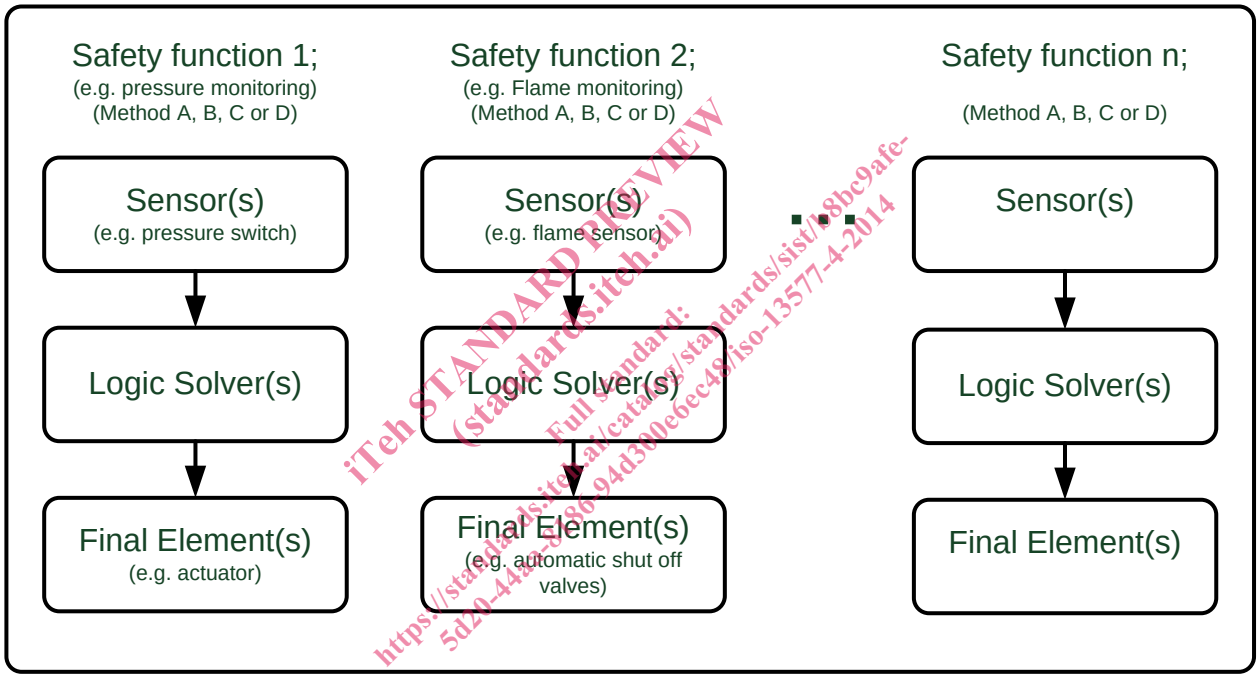

Figure 2 — Basic configuration of a protective system

Figure 3 is showing the basic characteristics of each method.

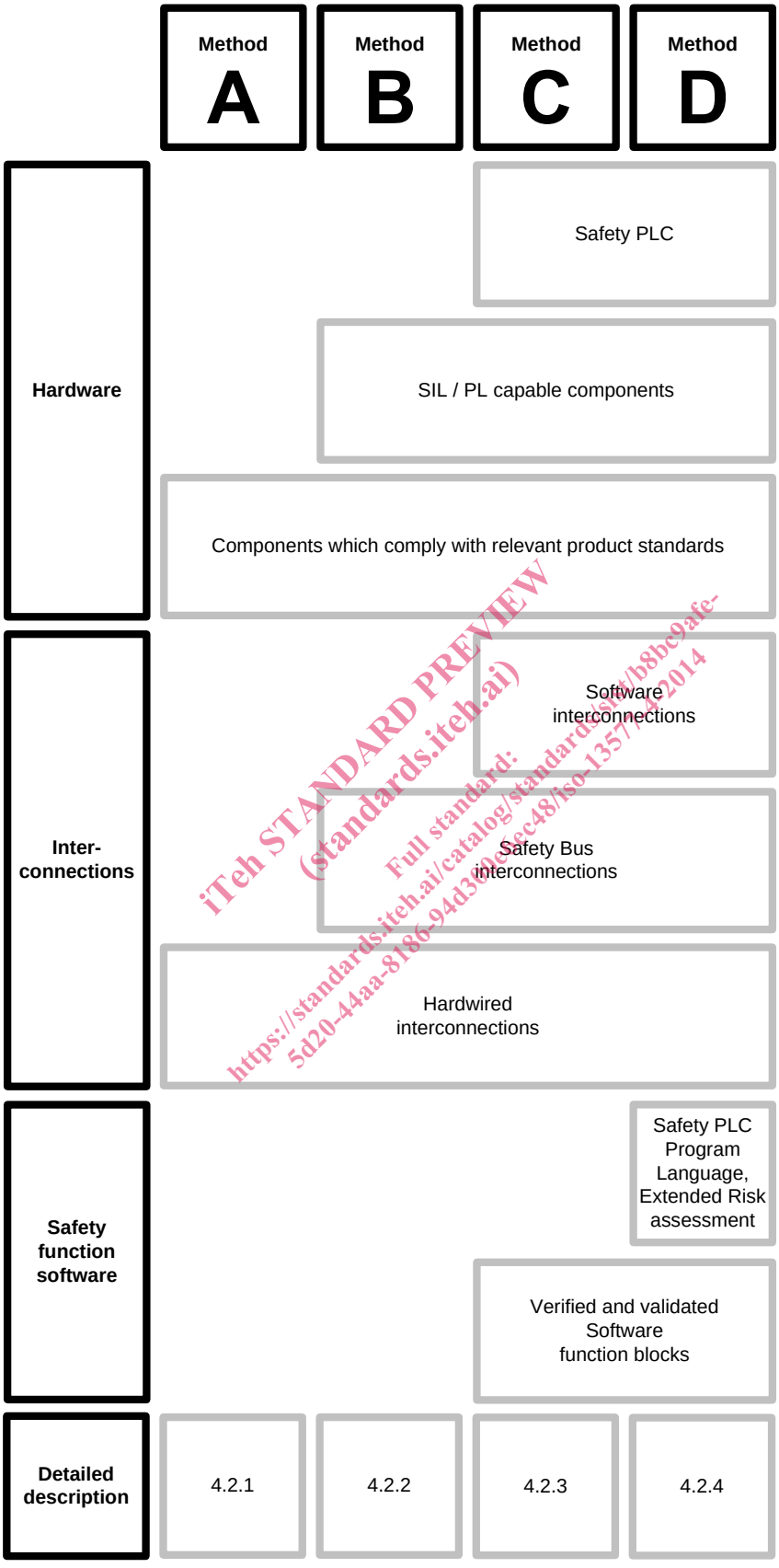

Figure 3 — Method overview

See informative Annex E for example schematics by 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 other parts of ISO 13577.

The requirements of IEC 61508, IEC 61511, IEC 62061 and ISO 13849 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 via the direct interconnections between the devices;

— connections shall not be permitted via data communication buses;

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

— be in accordance with Annex F.

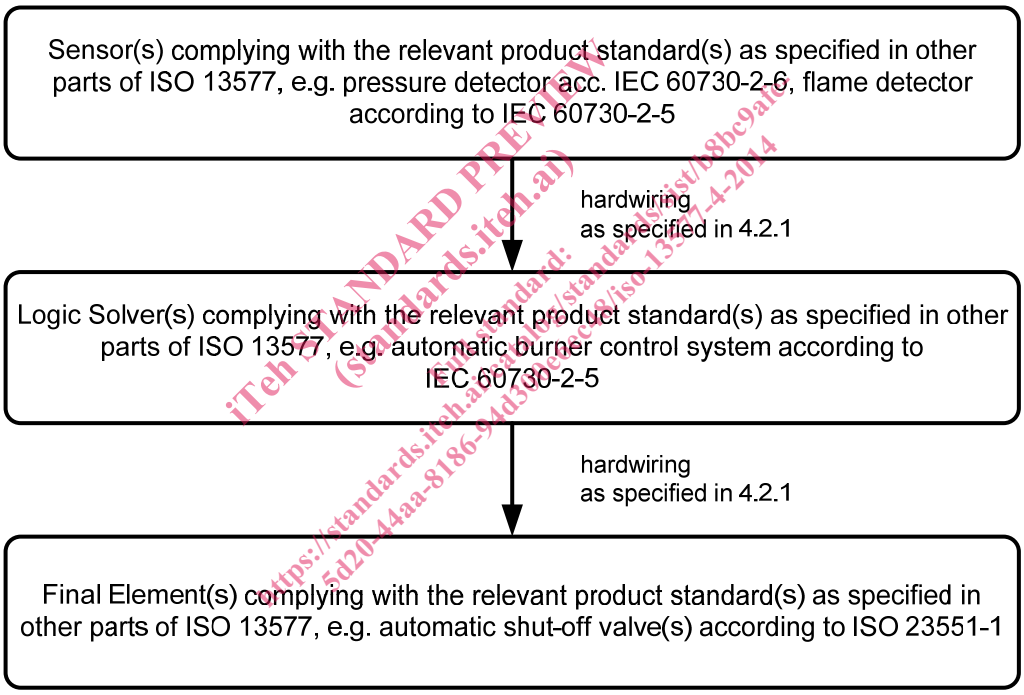

Figure 4 — Hardware configuration of Method A

NOTE The safety devices used here 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 per clause 4.1.1) must thus be viewed as 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 via the direct interconnections between the devices.