

JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS B 8415-3 : 2020

(JIFMA/JSA)

**General safety code for industrial
combustion furnaces — Part 3: Protective
systems**

This document has incorporated the erratum to the Japanese version
issued in July, 2021.

ICS 13.100 ; 25.180.01

Reference number : JIS B 8415-3 : 2020 (E)

PROTECTED BY COPYRIGHT

Date of Establishment: 2020-03-23

Date of Public Notice in Official Gazette: 2020-03-23

Investigated by: Japanese Industrial Standards Committee
Standards Board for ISO area

JIS B 8415-3 : 2020, First English edition published in 2021-08

Translated and published by: Japanese Standards Association
Mita MT Building, 3-13-12, Mita, Minato-ku, Tokyo, 108-0073 JAPAN

In the event of any doubts arising as to the contents,
the original JIS is to be the final authority.

© JSA 2021

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

Printed in Japan

PROTECTED BY COPYRIGHT

HT/HN

 **Documents**
Document Sharing Hub

Contents

	Page
Introduction	1
1 Scope	2
2 Normative references	2
3 Terms and definitions	3
4 Design requirements for equipment in a protective system	7
4.1 General	7
4.2 Requirements for protective systems	8
4.3 Fault assessment for the hardwired section of protective systems	21
4.3A Fault assessment for the hardwired section of the logic solver conform- ing to 4.2.5	21
4.4 Failure of utilities	21
4.5 Reset	21
Annex A (informative) Explanation of techniques and measures for avoiding systematic faults	23
Annex B (informative) Examples of techniques for avoiding failures from external wiring	25
Annex C (informative) Examples for the determination of safety integrity level SIL using the risk graph method	29
Annex D (informative) Example of an extended risk assessment for one safety instrumented function using the JIS C 0511 method	50
Annex E (informative) Sample schematic diagrams of protective system	59
Annex F (normative) Hardwiring protective systems	69
Annex JA (informative) Example of inspection points of combustion furnace	80
Annex JB (informative) Relevant product standards specified in JIS B 8415-2 and ISO 13577-2	84
Annex JC (informative) Bibliography	86
Annex JD (informative) Comparison table between JIS and corresponding International Standard	88

Foreword

This Japanese Industrial Standard has been established by the Minister of Economy, Trade and Industry through deliberations at the Japanese Industrial Standards Committee according to the proposal for establishment of Japanese Industrial Standard submitted by Japan Industrial Furnace Manufacturers Association (JIFMA)/Japanese Standards Association (JSA) with a draft being attached, based on the provision of Article 12, paragraph (1) of the Industrial Standardization Act. This Standard partially replaces **JIS B 8415**:2008, which has been withdrawn.

This **JIS** document is protected by the Copyright Act.

Attention is drawn to the possibility that some parts of this Standard may conflict with patent rights, published patent application or utility model rights. The relevant Minister and the Japanese Industrial Standards Committee are not responsible for identifying any of such patent rights, published patent application or utility model rights.

JIS B 8415 series consists of the following 3 parts under the general title *General safety code for industrial combustion furnaces* — :

Part 1: General requirements

Part 2: Combustion and fuel handling systems

Part 3: Protective systems

General safety code for industrial combustion furnaces — Part 3 : Protective systems

Introduction

This Japanese Industrial Standard has been prepared based on **ISO 13577-4** : 2014, Edition 1, with some modifications of the technical contents to corresponding to the actual situations in Japan.

The vertical lines on both sides and dotted underlines indicate changes from the corresponding International Standard. A list of modifications with the explanations is given in Annex JD. Annex JA, Annex JB and Annex JC are unique to **JIS** and not given in the corresponding International Standard.

This Standard was developed to specify the requirements of a protective system, which is a safety-related electrical control system (SRECS) of industrial combustion furnaces and associated devices (hereafter referred to as the combustion furnaces).

Mandatory safety-related control functions of combustion furnaces are specified in other parts of **JIS B 8415**.

It is intended that in designing the protective system of combustion furnaces, manufacturers of combustion furnaces choose from the four methods provided in this Standard.

This Standard is a type-C standard as defined in **JIS B 9700**.

This Standard is to be used together with the other parts of **JIS B 8415**. Since **JIS B 8415** series is a type-C standard of **JIS B 9700**, the combustion furnaces are required to be designed in accordance with the principles of **JIS B 9700**. However, there are cases in which a risk assessment according to **JIS C 0511** is more suitable for the design of a combustion furnace protective system. The machinery concerned and the extent to which hazards, hazardous situations or hazardous events are covered are indicated in the scope of this Standard.

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.

JIS C 0511 provides the option of a low-demand rate (system for permanent operation) on the protective system. **JIS B 9961** and **JIS B 9705-1** always assume high-demand rate (system for non-permanent operation) applications. Therefore, this Standard permits extended risk assessment for SRECS in which risk assessment based on **JIS C 0511** may be chosen as an alternative.

1 Scope

This Standard specifies the requirements for protective systems used in industrial combustion furnaces and associated devices.

The safety functional requirements to which the protective systems apply are specified in Part 1 and Part 2 of **JIS B 8415**.

NOTE The International Standard corresponding to this Standard and the symbol of degree of correspondence are as follows.

ISO 13577-4 : 2014 *Industrial furnace and associated processing equipment — Safety — Part 4 : Protective systems* (MOD)

In addition, symbols which denote the degree of correspondence in the contents between the relevant International Standard and **JIS** are IDT (identical), MOD (modified), and NEQ (not equivalent) according to **ISO/IEC Guide 21-1**.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. The most recent editions of the standards (including amendments) indicated below shall be applied.

JIS B 3503 *Programmable controllers — Programming languages*

NOTE Corresponding International Standard : IEC 61131-3 *Programmable controllers — Part 3 : Programming languages*

JIS B 9705-1 *Safety of machinery — Safety-related parts of control systems — Part 1 : General principles for design*

NOTE Corresponding International Standard : ISO 13849-1 *Safety of machinery — Safety-related parts of control systems — Part 1 : General principles for design*

JIS B 9960-1 *Safety of machinery — Electrical equipment of machines — Part 1 : General requirements*

NOTE Corresponding International Standard : IEC 60204-1 *Safety of machinery — Electrical equipment of machines — Part 1 : General requirements*

JIS B 9961 *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

NOTE Corresponding International Standard : IEC 62061 *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*

JIS C 0508 (all parts) *Functional safety of electrical/electronic/programmable electronic safety-related systems*

NOTE Corresponding International Standard : IEC 61508 (all parts) *Functional safety of electrical/electronic/programmable electronic safety-related systems*

JIS C 0511 (all parts) *Functional safety — Safety instrumented systems for the*

process industry sector

NOTE Corresponding International Standard : IEC 61511 (all parts) *Functional safety—Safety instrumented systems for the process industry sector*

JIS C 8201-4-1 *Low-voltage switchgear and controlgear — Part 4-1 : Contactors and motor-starters : Electromechanical contactors and motor-starters*

NOTE Corresponding International Standard : IEC 60947-4-1 *Low-voltage switchgear and controlgear — Part 4-1 : Contactors and motor-starters — Electromechanical contactors and motor-starters*

JIS C 8201-5-1 *Low-voltage switchgear and controlgear — Part 5-1 : Control circuit devices and switching elements — Electromechanical control circuit devices*

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

JIS C 9730-2-5 *Automatic electrical controls for household and similar use — Part 2-5 : Particular requirements for automatic electrical burner control systems*

NOTE Corresponding International Standard : IEC 60730-2-5 *Automatic electrical controls — Part 2-5 : Particular requirements for automatic electrical burner control systems*

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

3 Terms and definitions

For the purpose of this Standard, the terms and definitions given in **ISO 13574**, and the following apply.

3.1

automatic shut-off valve

valve that opens when energised and closes automatically when de-energized to shut off the fuel supply

NOTE See **2.194** of **ISO 13574**.

3.2

final element

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

NOTE 1 Valves, switchgears, motors including their auxiliary elements, for example, a solenoid valve and actuator if involved in the safety function.

NOTE 2 The definition in **3.2.22** of **JIS C 0511-1** is partially modified, and “safety instrumented system” is changed to “protective system”.

3.3

flame detector device

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

NOTE 1 It can consist of a flame sensor, a flame detector amplifier and a relay for signal transmission.

NOTE 2 The definition in **2.65** of **ISO 13574** is modified, and NOTE is added.

3.4

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 See **2.73** of **ISO 13574**.

3.5

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 Logic functions are executed by the logic solver (**3.6**) of a protective system.

NOTE 2 The definition in **3.2.35** of **JIS C 0511-1** is modified, and “input functions” is changed to “input functions or sensors” and “output functions” is changed to “output functions or final elements”.

3.6

logic solver

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

NOTE 1 For example, electrical systems, electronic systems, programmable electronic systems, pneumatic systems and hydraulic systems are available. Sensors and final elements are not part of the logic solver.

NOTE 2 NOTE 1 in **3.2.36** of **JIS C 0511-1** is deleted, and “either a BPCS or SIS” in the definition is changed to “a protective system”.

3.7

manual reset

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

NOTE See **2.107** of **ISO 13574**.

3.8

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

NOTE See 3.1.23 of JIS B 9705-1.

3.9

product standard

standard for products and components which are listed in all parts of JIS B 8415 except this Standard

NOTE See 2.135 of ISO 13574.

3.10

programmable logic control (PLC)

digitally operating electronic system which uses a programmable memory for the internal storage of user-oriented instructions for the implementation of specific control function as the control of various machines and processes through digital or analogue inputs/outputs

NOTE See 2.125 of ISO 13574.

3.11

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 (see Figure 2)

NOTE 1 The protective system can include either safety-related instrumented control functions and/or safety related-instrumented protection functions.

NOTE 2 See 2.138 of ISO 13574.

3.12

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 accordance with JIS C 0508 (all parts) or JIS C 9730-2-5

NOTE See 2.164 of ISO 13574.

3.13

safety device

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

NOTE For example, sensors, limiters, flame supervision devices, burner control systems, logic systems, final elements and automatic shut-off valves are available.

3.14

safety integrity level (SIL)

discrete level (one out of four) corresponding to a range of safety integrity values

- NOTE 1 Safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.
- NOTE 2 The target failure measures for the four safety integrity levels are specified in Table 2 and Table 3 of **JIS C 0508-1**.
- NOTE 3 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 4 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 .
- NOTE 5 See **3.5.8** of **JIS C 0508-4**.

3.15

sensor

device that produces a signal based on a process variable

- NOTE For example, Transmitters, transducers, process switches and position switches are available.

3.16

system for permanent operation

system intended to remain in the operating state for longer than 24 h without interruption

- NOTE In this Standard, the meaning of “permanent operation” is “continuous operation” commonly used in the field of industrial combustion furnaces, which is different from that specified in 2.5.101 of JIS C 9730-2-5.

3.17

system for non-permanent operation

system intended to remain in the operating state for less than 24 h

- NOTE In this Standard, the meaning of “non-permanent operation” is “non-continuous operation” commonly used in the field of industrial combustion furnaces, which is different from that specified in 2.5.102 of JIS C 9730-2-5.

3.18

systematic capability

measure 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 Expressed on a scale of SC1 to SC4.

NOTE 2 Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see **JIS C 0508-2** and **JIS C 0508-3**).

NOTE 3 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 4 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.

NOTE 5 See **2.183** of **ISO 13574**.

4 Design requirements for equipment in a protective system

4.1 General

Electrical equipment shall comply with **JIS B 9960-1** 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 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.

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

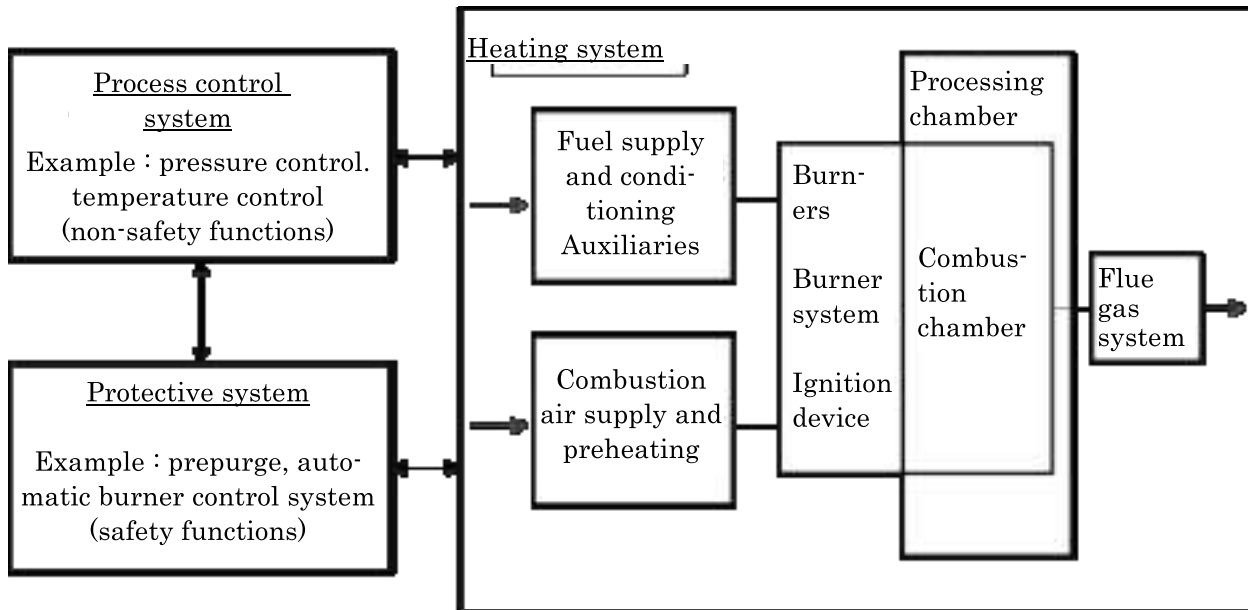


Figure 1 Block diagram of control and protective systems

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 specified in 4.2.4, 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.

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

4.2 Requirements for protective systems

4.2.0A General

Any one or a combination of the four methods shall be used to implement a protective system for the safety function(s) requirements specified in all parts of **JIS B 8415** including this Standard; however, only one method shall be used for any one specific safety function. The four methods are the following :

- Method A (specified in 4.2.1);
- Method B (specified in 4.2.2);
- Method C (specified in 4.2.3);
- Method D (specified in 4.2.4).

Figure 2 shows the basic configuration of a protective system.

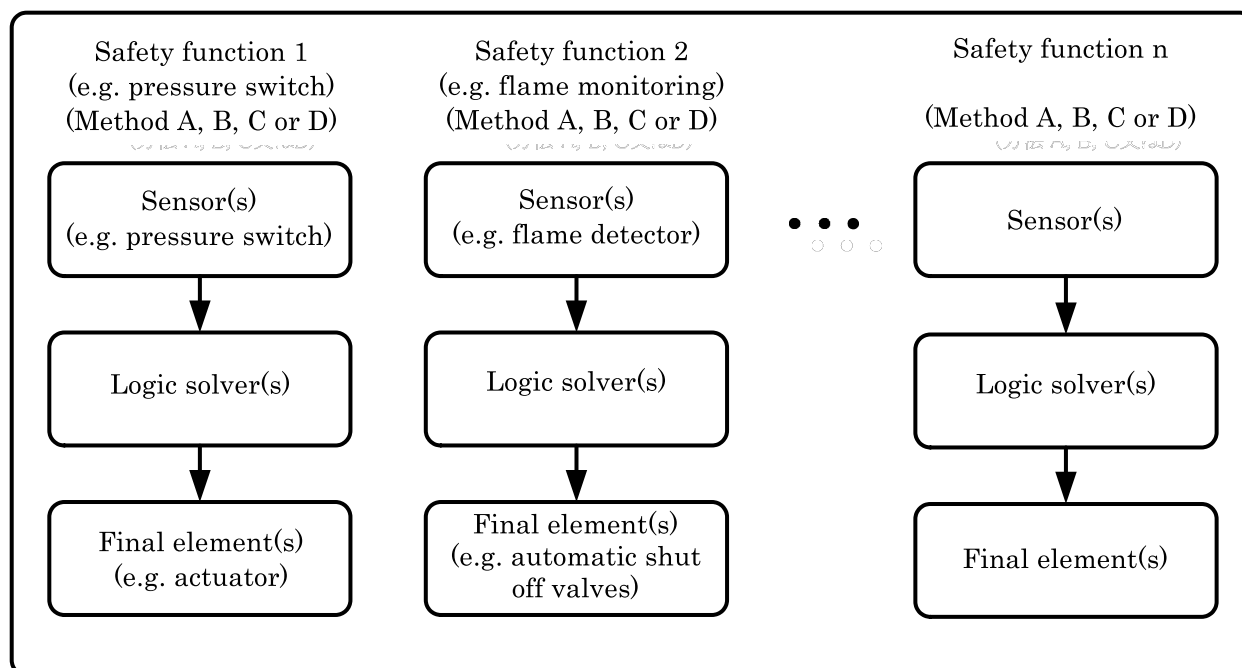


Figure 2 Basic configuration of a protective system

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 hard-wired interconnections between devices.
- NOTE 2 Safety function software is any of a software function block or program to perform safety logic functions (e.g. prepurge, automatic burner control).

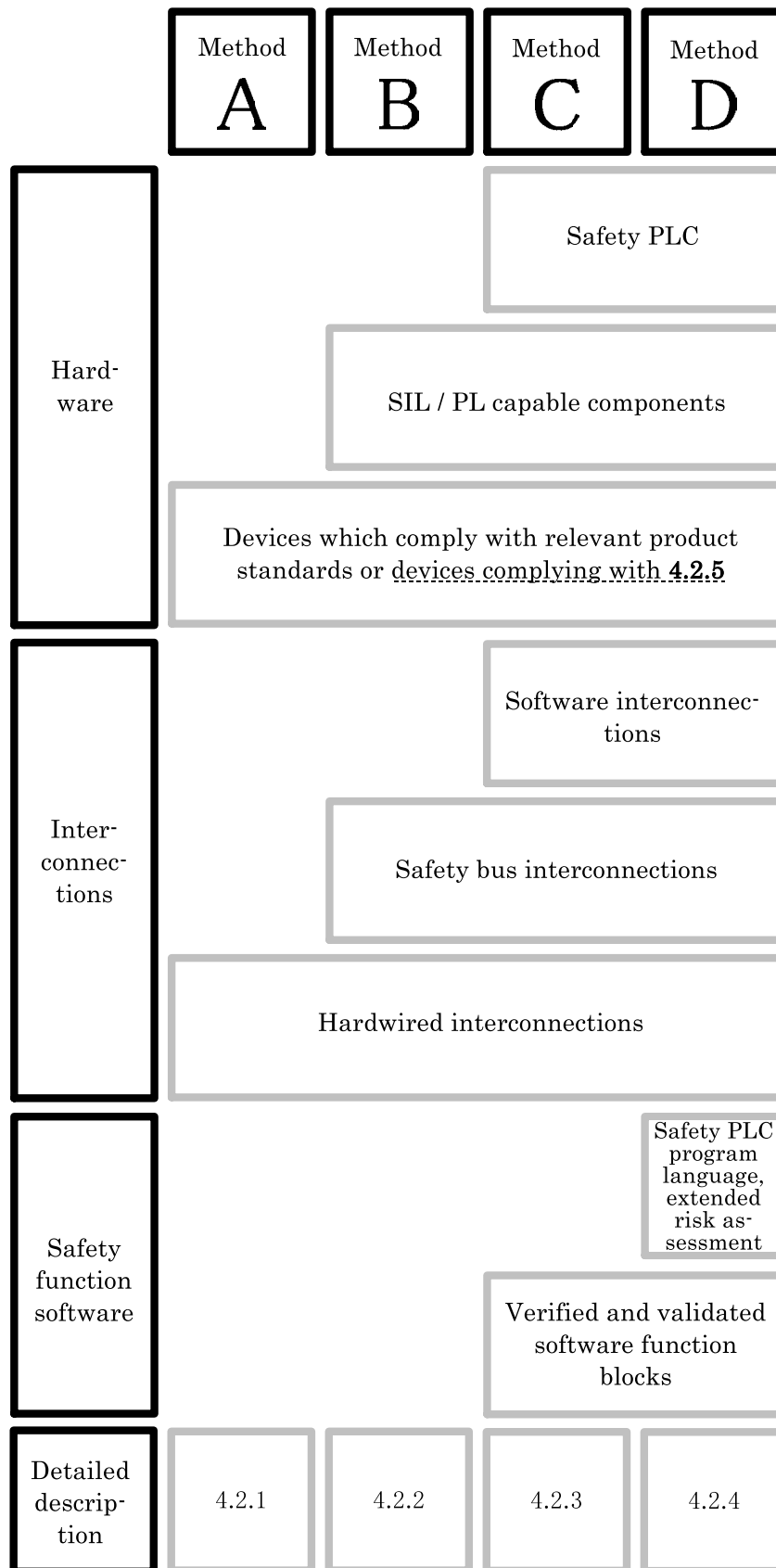


Figure 3 Method overview

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 solvers and final elements described in Figure 4) comply with the relevant product standards as specified in **JIS B 8415** (all parts) (see Annex JB).

The requirements of **JIS C 0508** (all parts), **JIS C 0511** (all parts), **JIS B 9961** and **JIS B 9705-1** 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.

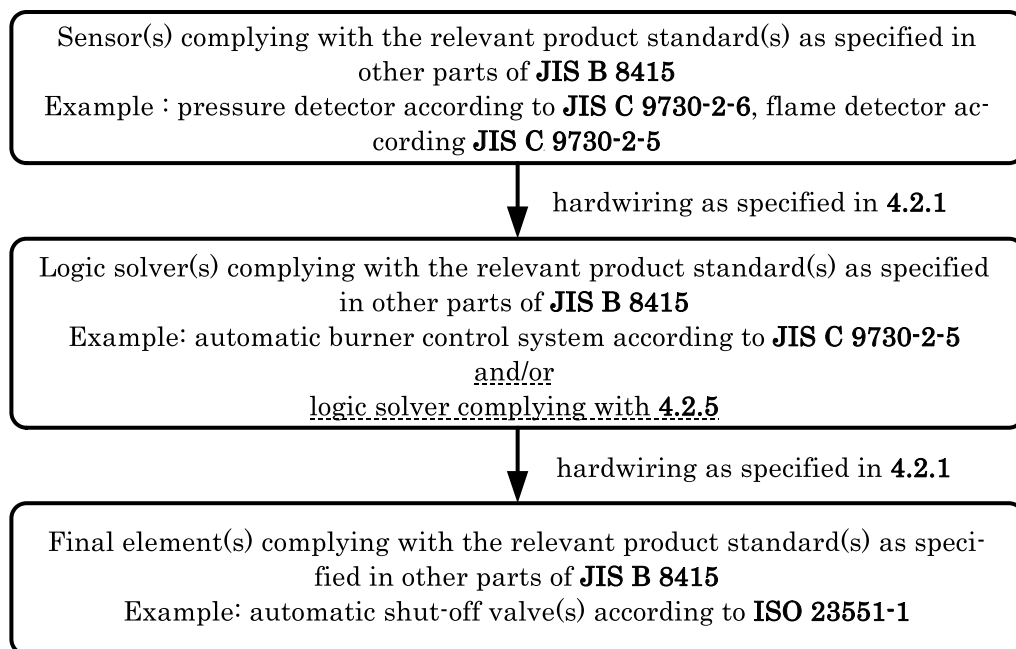


Figure 4 Hardware configuration of Method A

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 exists. 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 between elements 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 devices shall be SIL3 capable in accordance with **JIS C 0508** (all parts), **JIS B 9961** and **JIS C 0511** (all parts) or it shall be PLe capable in accordance with **JIS B 9705-1**;
- 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 **JIS Q 17025**.

Devices with less than SIL3/PLe 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 **JIS C 0511** (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.

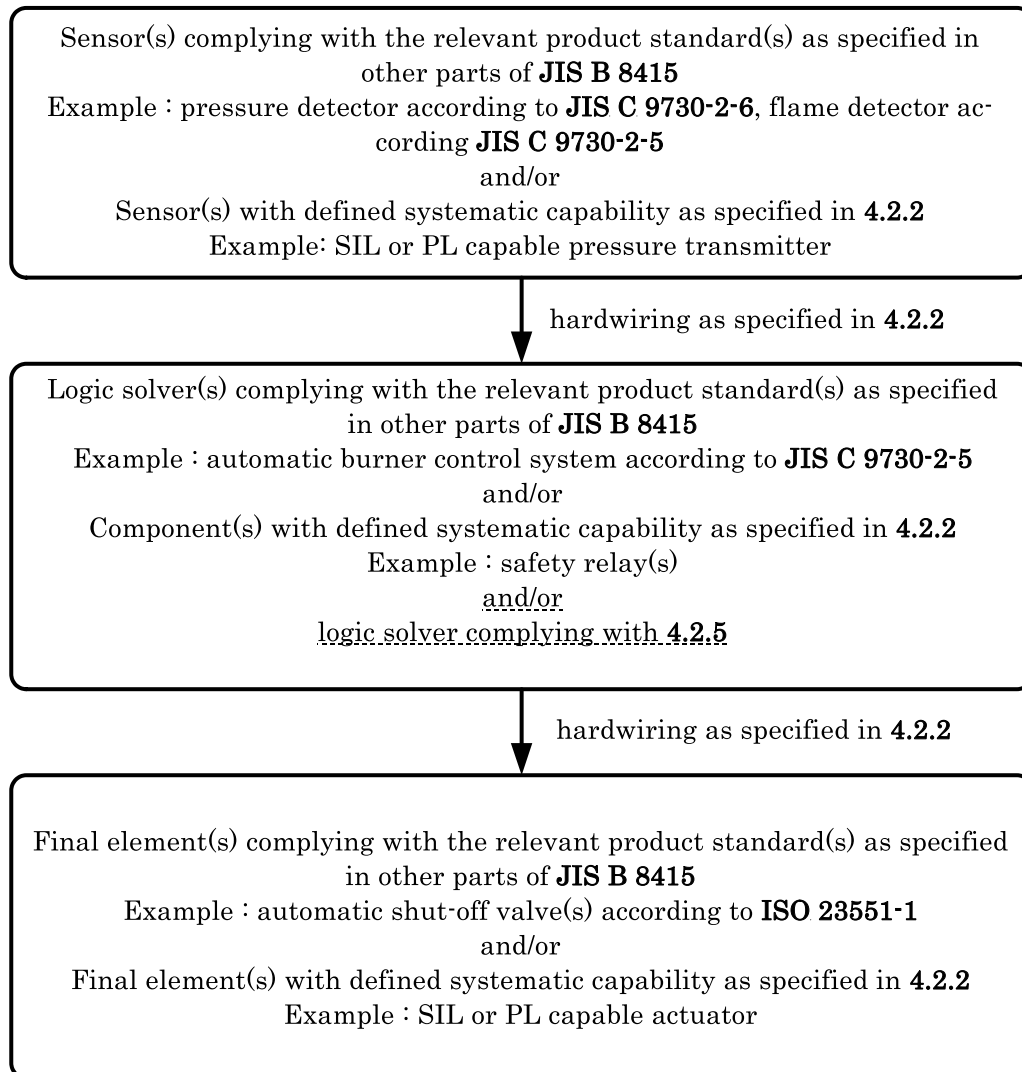


Figure 5 Hardware configuration of Method B

4.2.3 Method C

4.2.3.A General

Method C shall be a combination of devices meeting the relevant product standards (see Annex JB) and/or SIL/PL capable devices for which no relevant product standard exists 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;
- interconnections between elements shall be any of 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 SIL3 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 SIL3 capable in accordance with **JIS C 0508** (all parts), **JIS B 9961** and **JIS C 0511** (all parts) or it shall be PLe capable in accordance with **JIS B 9705-1**;
- 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 **JIS B 3503**;
- software shall be locked and secured against unauthorized and unintentional changes.

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 **JIS Q 17025**.

Devices with less than SIL3/PLe 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 **JIS C 0511** (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.

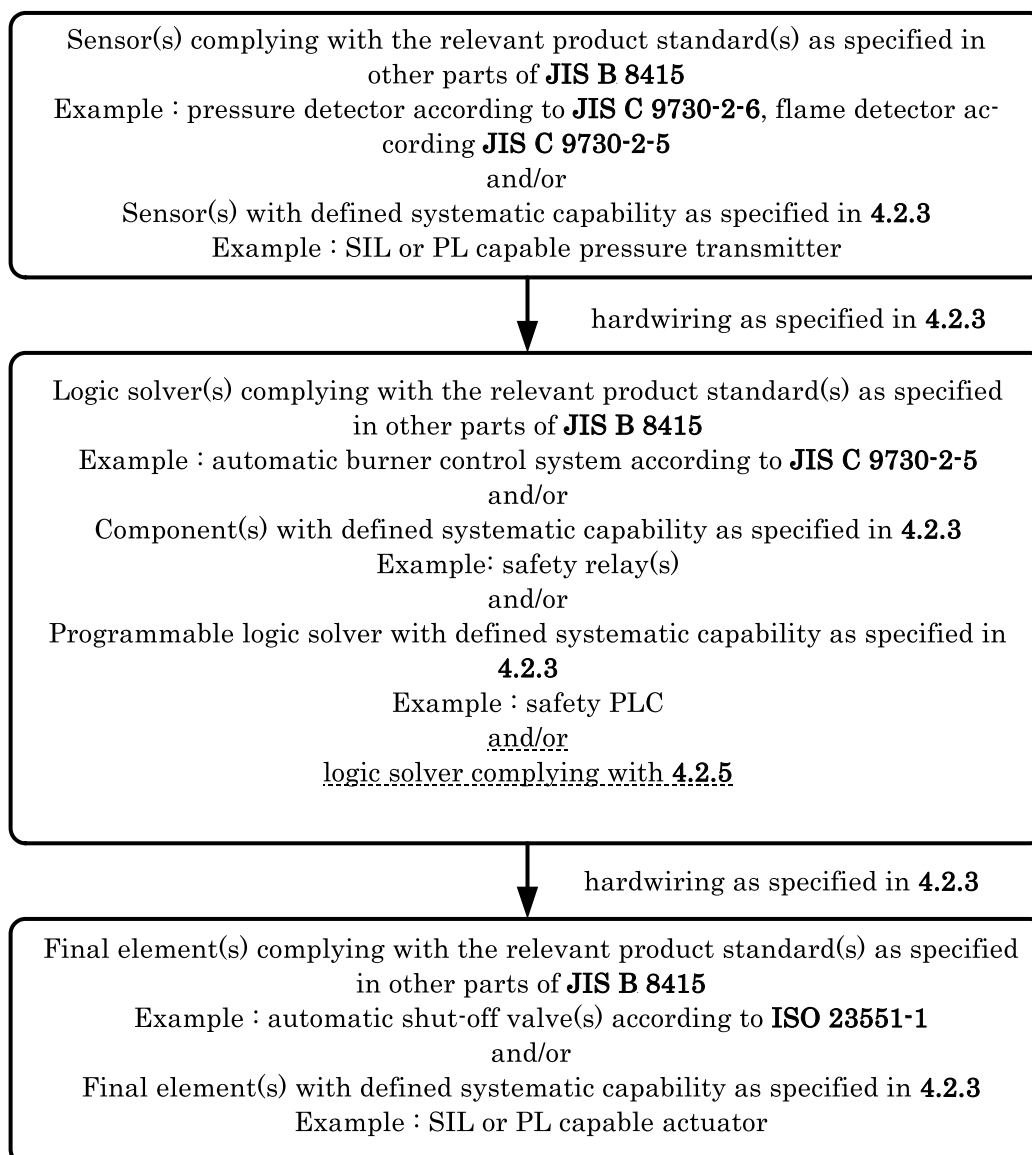


Figure 6 Hardware configuration of Method C

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 device 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 **JIS C 0508** (all parts), **JIS B 9961**, **JIS C 0511** (all parts) or **JIS B 9705-1** (see Figure 7).

NOTE See Annex D for the method in accordance with **JIS C 0511** (all parts).

Method D shall also fulfil the following requirements :

- a) the flame detector shall comply with **JIS C 9730-2-5**;
- 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 testing frequency requirements;
- c) each functional safety requirement, as identified in other parts of **JIS B 8415**, shall be evaluated for its need in accordance with the standards, such as **JIS C 0508** (all parts), **JIS B 9961**, **JIS C 0511** (all parts) or **JIS B 9705-1**, 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 fulfil 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 **JIS B 8415** (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 this Standard.

- d) interconnections between elements shall be any of 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 in accordance with **JIS Q 17025**.

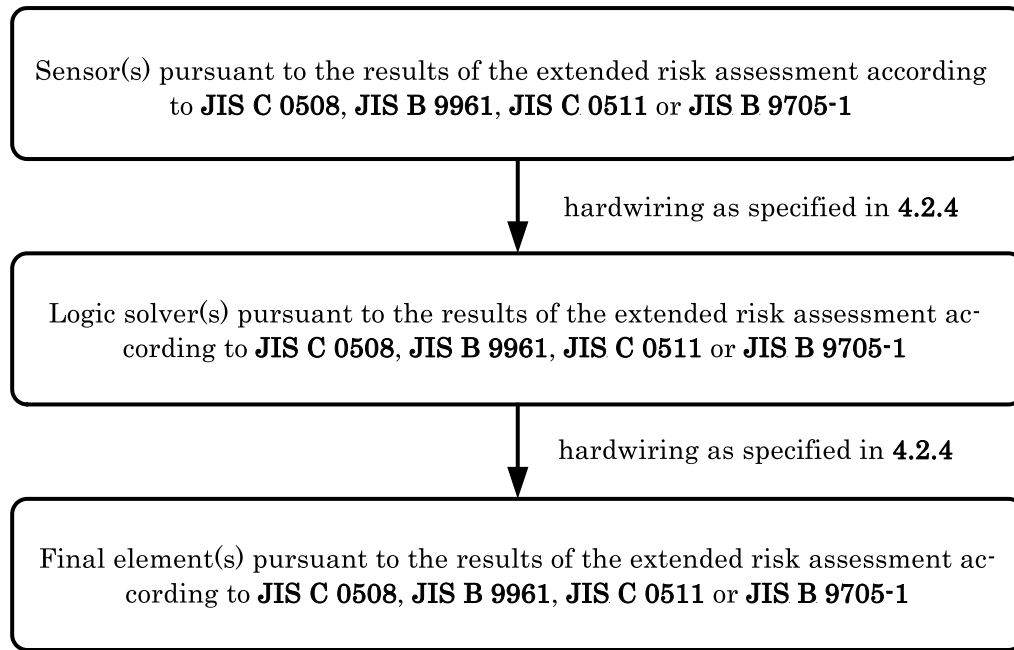


Figure 7 Hardware configuration of Method D

4.2.5 Devices applicable to logic solver of Method A, Method B and Method C

4.2.5.1 General

The devices composed of the control circuit and the operating circuit in accordance with 4.2.5.2, 4.2.5.3, 4.2.5.4, 4.2.5.5 and 4.2.5.6 may be treated as the devices equivalent to the logic solver composed of instruments specified by the relevant product standards. This logic solver is applicable to Method A, Method B and Method C.

4.2.5.2 General requirements

General requirements shall be as follows

- a) For the component parts of devices, their structure, performance and characteristic shall withstand mechanically, chemically and thermally during the working period intended.
- b) The devices shall correctly work at all operational pressures, at ambient temperature 0 °C to 40 °C, and with range of supply voltage variation $\pm 10\%$. However, for the machinery installed and used at any environment different from this, an adequate machinery shall be selected. When the ambient temperature exceeds the maximum working temperature of the machinery, the environment where the temperature of machinery cannot rise shall be prepared by using a cooling device or heat shut-off device.
- c) The control parts subjected to pressure shall withstand the mechanical stress and thermal stress causing such deformation as compromising safety.
- d) The devices shall be protected from the influence of the heat release from industrial furnace equipment and combustion machinery, and incorrect operation.

- e) The devices shall be safely operated and shall be protected against the possibility that the operation result becomes an unsafe action.
- f) The combustion safeguard shall be provided with the function to shut off the fuel supply immediately in the events of shut-off of the operational power source, or disconnection of the electric wiring.
- g) When the industrial furnace equipment is stopped by the safety failure and the combustion safeguard, and then recovers to the normal conditions, it shall not automatically restart; restart shall only be activated by the starting switch after removal of the abnormality and confirmation of the safety.
- h) The safety devices shall not be allowed that the function is easily lost. The use of safety devices detached or the function bypassed is not permissible.
- i) The inspection procedures and intervals of the safety functions should be prepared based on Annex JA.
- j) The effect from faults of component parts shall be examined in the design stage. The control system shall be constructed so that any fault of the control parts does not result in a hazardous situation.

4.2.5.3 Control circuit and operation circuit

For the control circuit and operation circuit, the essential safety design measures based on risk assessment shall be taken. Furthermore, the following shall be satisfied.

- a) All points of contact as interlock shall be installed in series to the holding circuit of safety shut-off valve.
- b) All points of contact of shut-off shall be positioned at the non-earthing side of power source. Further, where required, the electrical leakage countermeasures such as electrical leakage breaker, both ends cutting of contact point shall be performed.
- c) The control and operation circuit, where required, shall give promptly the warning such as by lighting, warning sound in the case of abnormal condition.
- d) The function of the ignition safety time shall be composed of an independent timer circuit and diagnosis circuit.

4.2.5.4 Operating panel, etc.

The control panel and operating panel shall satisfy the following.

- a) The switches of the operating panel, etc. shall be arranged in the order of operation procedure to prevent the operator from incorrect operations.
- b) They shall be installed at a place where the ambient temperature is below the allowable temperature and where they cannot be damaged by explosion, contact with high temperature objects, falling objects and so on.
- c) They shall be constructed so as to allow an easy inspection.

4.2.5.5 Junction relay

The contact of safety device used for the interlock of combustion safety circuit shall

not intermediate a junction relay. In the following cases, however, the junction relay may be used, provided that the preventive measures against the incorrect operations of junction relay or the melting of contact are taken by providing the junction relay at every safety shut-off valve or releasing the interlock by the shut-off checking switch at the time of starting and ignition.

- a) Case where the load exceeds the capacity of contact of safety device.
- b) Case where it is required for the return to safety condition at the time of power source shut-off.
- c) Case where the safety circuit logic function is required.

4.2.5.6 Programmable logic control (PLC)

When a programmable logic control is used in the protective system, the following **a)** or **b)** shall be satisfied.

- a) The requirements specified in **4.2.3** shall be satisfied.
- b) The following 1) to 8) shall be satisfied.
 - 1) When the safety PLC is not used, the interlock of combustion safety only by software shall not be constructed. Herein, the safety PLC means the PLC certified officially which has the safety function specified in SIL2 or SIL3 of **JIS C 0508-1** or organizations in accordance with **JIS Q 17025**.
 - 2) For the combustion safety circuit constructed by safety programmable controller, the function of circuit and safety of circuit shall be proved and the measure shall be taken so that the circuit can not be easily changed once proved.
 - 3) For the flame monitor, the PLC shall not be used. Further, the function of ignition safety time shall have or construct the diagnosis circuit or the timer circuit being independent from the programmable controller shall be installed.
 - 4) The supplier of the application software of the PLC shall present the data to the user to prove that all of control operation circuits are in the condition to achieve the function.
 - 5) When the power source is shut off, the PLC shall not interfere with the device returning to the safe initial condition. When the power source has recovered, the safe condition shall be maintained.
 - 6) The urgency stop switch to shut off the device shall be provided so as to be independent from the PLC. The signal transmission of urgency stop shall not be constructed only by communication. The PLC shall return to the safe condition by receiving the signal of urgency stop and even after the urgency stop is released, the safe condition shall be maintained.
 - 7) All of the alternations of hardware and software shall be documented, maintained and stored at the job site.
 - 8) The PLC shall be provided with the diagnosis function such as CPU and memory, and at the time of the failure of hardware and the abnormal action or breaking of

software, it shall have the system recover to the safe initial condition.

4.3 Fault assessment for the hardwired section of protective systems

The protective system shall be designed such that the devices required in **JIS B 8415** (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 **JIS C 8201-5-1** or the requested SIL/PL requirement. Power relays for safety with or without mirror contacts shall be in accordance with **JIS C 8201-4-1** or the requested SIL/PL requirement.
- b) The device shall be wired in accordance with the manufacturer's instructions.
- c) For Method B and Method C, when timers not complying with the relevant product standards as specified in all the other parts of **JIS B 8415** are used in safety functions, timers shall have a systematic capability of SC3 (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 under 60 % of the lowest device contact rating.
- e) Additional requirements shall be as given in Annex F.

4.3A Fault assessment for the hardwired section of the logic solver conforming to 4.2.5

The requirements of **a) to e)** in **4.3** shall not apply to the logic solver conforming to **4.2.5**. However, the assessment of conformity to the requirements of **4.2.5.2 j)** should be evaluated based on Annex F is preferable.

4.4 Failure of utilities

Loss of utilities (e.g. electrical power, instrument air) to the combustion furnaces 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 **4.2.7** or **4.3.7** of **JIS B 8415-2**).

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 **3.7**).

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 combustion furnaces.

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 combustion furnaces, 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 devices 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
 - the process application,
 - the applicable technology used (e.g. electrical, electronic, programming), and
 - 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 **JIS C 0511-1**.

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 **JIS C 0508-2**.

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;
 - 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 :

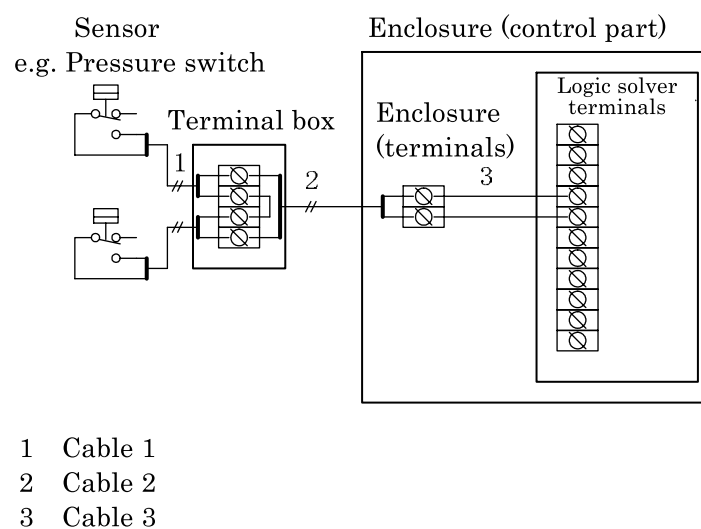
- a) the types of tests to be performed and procedures to be followed;
- b) the test environment, tools, configuration and programs;
- c) the pass/fail criteria.

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.



1 Cable 1
2 Cable 2
3 Cable 3
NOTE This diagram shows an improper example of external wiring practice.

Figure B.1 Improper external wiring method

Figure B.2 shows a technique that can provide a sufficient level of protection for the safety function when used with protective system Method A and Method 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.

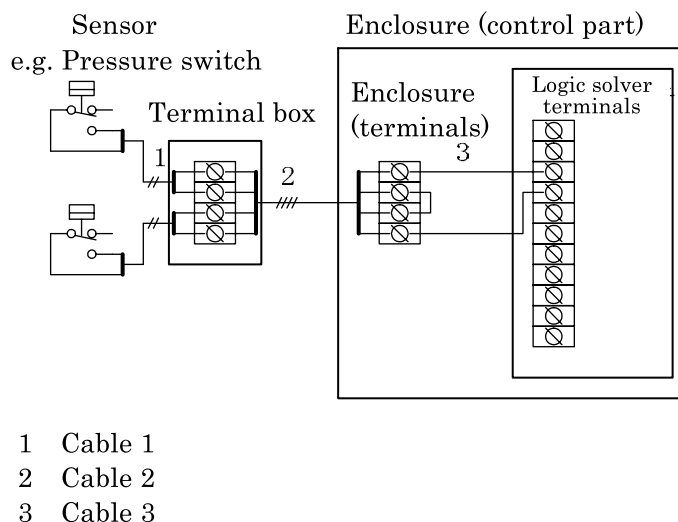


Figure B.2 Protected wiring

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 Method A, Method B, Method C or Method D.

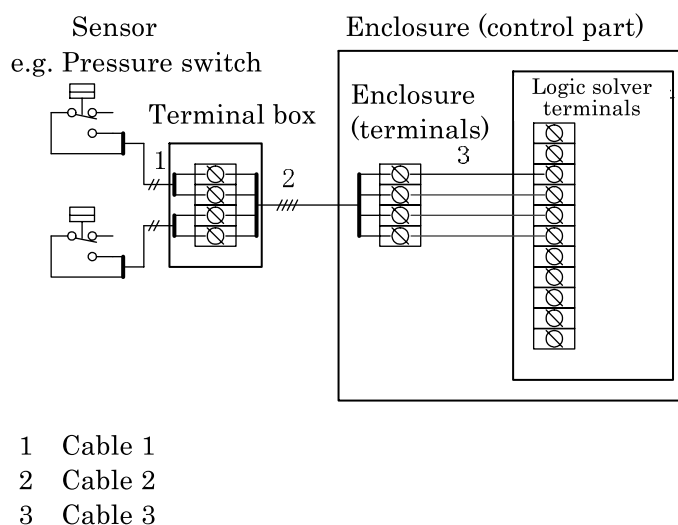


Figure B.3 Protected wiring, all conductors carried throughout

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 Method A, Method B, Method C or Method D.