

Functional safety — Safety instrumented systems for the process industry sector —

Part 2: Guidelines for the application of IEC 61511-1

The European Standard EN 61511-2:2004 has the status of a
British Standard

ICS 13.110; 25.040.01

National foreword

This British Standard is the official English language version of EN 61511-2:2004. It is identical with IEC 61511-2:2003.

The UK participation in its preparation was entrusted by Technical Committee GEL/65, Measurement and control, to Subcommittee GEL/65/1, System considerations, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the EN title page, pages 2 to 70, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments
15577	11 May 2005	Implementation of the European Standard

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 4 August 2003

© BSI 11 May 2005

ISBN 0 580 42376 X

EUROPEAN STANDARD

EN 61511-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

December 2004

ICS 25.040.01;13.110

English version

**Functional safety –
Safety instrumented systems for the process industry sector
Part 2: Guidelines for the application of IEC 61511-1
(IEC 61511-2:2003)**

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité
pour le secteur des industries
de transformation
Partie 2: Lignes directrices pour
l'application de la CEI 61511-1
(CEI 61511-2:2003)

Funktionale Sicherheit -
Sicherheitstechnische Systeme
für die Prozessindustrie
Teil 2: Anleitungen zur Anwendung
des Teils 1
(IEC 61511-2:2003)

This European Standard was approved by CENELEC on 2004-10-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Central Secretariat: rue de Stassart 35, B - 1050 Brussels

© 2004 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

Foreword

The text of the International Standard IEC 61511-2:2003, prepared by SC 65A, System aspects, of IEC TC 65, Industrial-process measurement and control, was submitted to the Unique Acceptance Procedure and was approved by CENELEC as EN 61511-2 on 2004-10-01 without any modification.

The following dates were fixed:

- latest date by which the EN has to be implemented
at national level by publication of an identical
national standard or by endorsement (dop) 2005-10-01
- latest date by which the national standards conflicting
with the EN have to be withdrawn (dow) 2007-10-01

Endorsement notice

The text of the International Standard IEC 61511-2:2003 was approved by CENELEC as a European Standard without any modification.

CONTENTS

INTRODUCTION	5
1 Scope	7
2 Normative references.....	7
3 Terms, definitions and abbreviations.....	7
4 Conformance to this International Standard	7
5 Management of functional safety.....	8
5.1 Objective	8
5.2 Requirements	8
6 Safety lifecycle requirements	14
6.1 Objective	14
6.2 Requirements	14
7 Verification	14
7.1 Objective	14
8 Process hazard and risk assessment	15
8.1 Objectives	15
8.2 Requirements	15
9 Allocation of safety functions to protection layers.....	18
9.1 Objective	18
9.2 Requirements of the allocation process	18
9.3 Additional requirements for safety integrity level 4	20
9.4 Requirement on the basic process control system as a layer of protection	20
9.5 Requirements for preventing common cause, common mode and dependent failures	22
10 SIS safety requirements specification	22
10.1 Objective	22
10.2 General requirements	22
10.3 SIS safety requirements.....	22
11 SIS design and engineering	23
11.1 Objective	23
11.2 General requirements	23
11.3 Requirements for system behaviour on detection of a fault	27
11.4 Requirements for hardware fault tolerance.....	27
11.5 Requirements for selection of components and subsystems	29
11.6 Field devices	31
11.7 Interfaces	31
11.8 Maintenance or testing design requirements	33
11.9 SIF probability of failure.....	34
12 Requirements for application software, including selection criteria for utility software.....	36
12.1 Application software safety lifecycle requirements	36
12.2 Application software safety requirements specification.....	39
12.3 Application software safety validation planning	41
12.4 Application software design and development.....	41

12.5	Integration of the application software with the SIS subsystem	48
12.6	FPL and LVL software modification procedures	48
12.7	Application software verification.....	49
13	Factory acceptance testing (FAT)	50
13.1	Objectives	50
13.2	Recommendations	50
14	SIS installation and commissioning.....	51
14.1	Objectives	51
14.2	Requirements	51
15	SIS safety validation	51
15.1	Objective	51
15.2	Requirements	51
16	SIS operation and maintenance	52
16.1	Objectives	52
16.2	Requirements	52
16.3	Proof testing and inspection.....	52
17	SIS modification.....	54
17.1	Objective	54
17.2	Requirements	54
18	SIS decommissioning.....	54
18.1	Objectives	54
18.2	Requirements	54
19	Information and documentation requirements.....	54
19.1	Objectives	54
19.2	Requirements	54
Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function		56
Annex B (informative) Typical SIS architecture development.....		57
Annex C (informative) Application features of a safety PLC		62
Annex D (informative) Example of SIS logic solver application software development methodology		64
Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver		68
Figure 1 – Overall framework of this standard		6
Figure 2 – BPCS function and initiating cause independence illustration		20
Figure 3 – Software development lifecycle (the V-model)		37
Figure C.1 – Logic solver		63
Figure E.1 – EWDT timing diagram		70
Table 1 – Typical Safety Manual organisation and contents		46

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards.

This International Standard addresses the application of safety instrumented systems for the Process Industries. It also deals with the interface between safety instrumented systems and other safety systems in requiring that a process hazard and risk assessment be carried out. The safety instrumented system includes sensors, logic solvers and final elements.

This International Standard has two concepts, which are fundamental to its application; safety lifecycle and safety integrity levels. The safety lifecycle forms the central framework which links together most of the concepts in this International Standard.

The safety instrumented system logic solvers addressed include Electrical (E)/Electronic (E)/ and Programmable Electronic (PE) technology. Where other technologies are used for logic solvers, the basic principles of this standard may also be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This International Standard is process industry specific within the framework of the IEC 61508 series.

This International Standard sets out an approach for safety lifecycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used. The objective of this standard is to provide guidance on how to comply with IEC 61511-1.

To facilitate use of this standard, the clause and subclause numbers provided are identical to the corresponding normative text in 61511-1 (excluding the annexes).

In most situations, safety is best achieved by an inherently safe process design whenever practicable, combined, if necessary, with a number of protective systems which rely on different technologies (for example, chemical, mechanical, hydraulic, pneumatic, electrical, electronic, thermodynamic (for example, flame arrestors), programmable electronic) which manage any residual identified risk. Any safety strategy considers each individual safety instrumented system in the context of the other protective systems. To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety functions and related safety systems, such as the safety instrumented system(s), is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This International Standard on safety instrumented systems for the process industry:

- addresses relevant safety lifecycle stages from initial concept, through design, implementation, operation and maintenance and decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

This standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

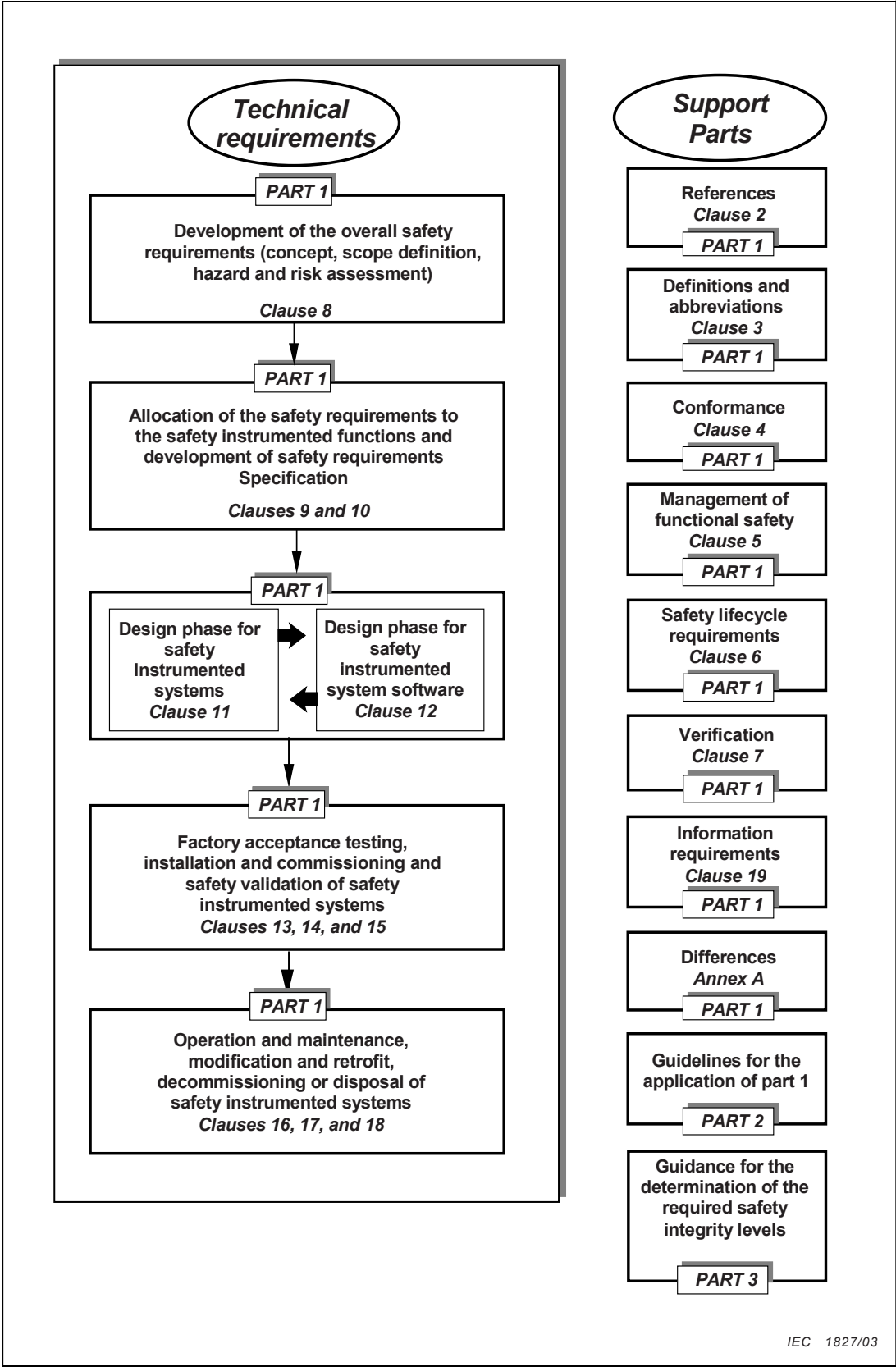


Figure 1 – Overall framework of this standard

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 2: Guidelines for the application of IEC 61511-1

1 Scope

IEC 61511-2 provides guidance on the specification, design, installation, operation and maintenance of Safety Instrumented Functions and related safety instrumented system as defined in IEC 61511-1. This standard has been organized so that each clause and subclause number herein addresses the same clause number in IEC 61511-1 (with the exception of the annexes).

2 Normative references

No further guidance provided.

3 Terms, definitions and abbreviations

No further guidance provided except for 3.2.68 and 3.2.71 of IEC 61511-1.

3.2.68 A safety function should prevent a specified hazardous event. For example, “prevent the pressure in vessel #ABC456 exceeding 100 bar.” A safety function may be achieved by

- a) a single safety instrumented system (SIS), or
- b) one or more safety instrumented systems and/or other layers of protection.

In case b), each safety instrumented system or other layer of protection has to be capable of achieving the safety function and the overall combination has to achieve the required risk reduction (process safety target).

3.2.71 Safety instrumented functions are derived from the safety function, have an associated safety integrity level (SIL) and are carried out by a specific safety instrumented system (SIS). For example, “close valve #XY123 within 5 s when pressure in vessel #ABC456 reaches 100 bar”. Note that components of a safety instrumented system may be used by more than one safety instrumented function.

4 Conformance to this International Standard

No further guidance provided.

5 Management of functional safety

5.1 Objective

The objective of Clause 5 of IEC 61511-1 is to provide requirements for implementing the management activities that are necessary to ensure that the functional safety objectives are met.

5.2 Requirements

5.2.1 General

5.2.1.1 No further guidance provided.

5.2.1.2 When an organization has responsibility for one or more activities necessary for functional safety and that organization works according to quality assurance procedures, then many of these activities described in this clause will already be carried out for the purposes of quality. Where this is the case, it may be unnecessary to repeat these activities for the purposes of functional safety. In such cases, the quality assurance procedures should be reviewed to establish that they are suitable so that the objectives of functional safety will be achieved.

5.2.2 Organization and resources

5.2.2.1 The organizational structure associated with safety instrumented systems within a Company/Site/Plant/Project should be defined and the roles and responsibilities of each element clearly understood and communicated. Within the structure, individual roles, including their description and purpose should be identified. For each role, unambiguous accountabilities should be identified; and specific responsibilities should be recognised. In addition, whom the individual reports to and who makes the appointment should be identified. The intent is to ensure that everyone in an organization understands their role and responsibilities for safety instrumented systems.

5.2.2.2 The skills and knowledge required to implement any of the activities of the safety life cycle relating to the safety instrumented systems should be identified; and for each skill, the required competency levels should be defined. Resources should be assessed against each skill for competency and also the number of people per skill required. When differences are identified, development plans should be established to enable the required competency levels to be achieved in a timely manner. When shortages of skills arise, suitably qualified and experienced personnel may be recruited or contracted.

5.2.3 Risk evaluation and risk management

The requirement stated in 5.2.3 of IEC 61511 is that hazards are identified, risks evaluated and the necessary risk reduction is determined. It is recognized that there are numerous different methodologies available for conducting these evaluations. IEC 61511-1 does not endorse any particular methodology. Instead, the reader is encouraged to review a number of methodologies on this issue in IEC 61511-3. See 8.2.1 for further guidance.

5.2.4 Planning

The intent of this subclause is to ensure that, within the overall project, adequate safety planning is conducted so that all of the required activities during each phase of the lifecycle (for example, engineering design, plant operation) are addressed. The standard does not require any particular structure for these planning activities, but it does require periodic update or review of them.

5.2.5 Implementing and monitoring

5.2.5.1 The intent of this subclause is to ensure that effective management procedures are in place to

- ensure that all recommendations resulting from hazard analysis, risk assessment, other assessment and auditing activities, verification and validation activities are satisfactorily resolved.
- determine that the SIS is performing in accordance with its safety requirements specification throughout its operational lifetime.

5.2.5.2 Note that, in this context, suppliers could include design contractors and maintenance contractors as well as suppliers of components.

5.2.5.3 A review of the SIS performance should be periodically undertaken to ensure the original assumptions made during the development of the safety requirements specification (SRS) are still adhered to. For example, a periodic review of the assumed failure rate of different components in a SIS should be carried out to ensure that it remains as originally defined. If the failure rates are worse than originally anticipated, a design modification may be necessary. Likewise, the demand rate on the SIS should be reviewed. If the rate is more than that which was originally assumed, then an adjustment in the SIL may be needed.

5.2.6 Assessment, auditing and revision

Assessments and audits are tools targeted at the detection and elimination of errors. The paragraphs below make clear the distinction between these activities

Functional safety assessment aims to evaluate whether provisions made during the assessed lifecycle phases are adequate for the achievement of safety. Judgements are made by assessors on the decisions taken by those responsible for the realisation of functional safety. An assessment would for example be made prior to commissioning as to whether procedures for maintenance are adequate.

Functional safety auditors will determine from project or plant records whether the necessary procedures have been applied at the specified frequency by persons with the necessary competence. Auditors are not required to make judgements on the adequacy of the work they are considering. However, if they became aware that there would be benefits in making changes, then an observation should be included in the report.

It should be noted that in many cases there can be an overlap between the work of the assessor and the auditor. For example an auditor may need to determine not only whether an operator has been given the necessary training but in addition make judgements as to whether the training has resulted in the required competency.

5.2.6.1 Functional safety assessment

5.2.6.1.1 The use of Functional Safety Assessment (FSA) is fundamental in demonstrating that a Safety Instrumented System (SIS) fulfils its requirements regarding safety instrumented function(s) and Safety Integrity Level (SIL). The basic objective of this assessment is to demonstrate compliance with agreed standards and practices through independent assessment of the system's development process. An assessment of a SIS may be needed at different lifecycle stages. In order to conduct an effective assessment, a procedure should be developed that defines the scope of this assessment along with some guidance on the makeup of the assessment team.

The following attributes are considered good practice for Functional Safety Assessment:

- A plan should be generated for each FSA identifying such arrangements as the scope of the assessment, the assessors, the competencies of the assessors and the information to be generated by the assessment.

- The FSA should take into account other standards and practices, which may be contained within external or internal corporate standards, guides, procedures or codes of practice. The FSA plan should define what is to be assessed for the particular assessment/system/application area.
- The frequency of FSAs may vary across different system developments but as a minimum should always take place before the potential hazards being presented to the system. Some companies also like to conduct an assessment prior to the construction/installation phase to prevent costly rework later in the lifecycle.
- FSA frequency and rigour should be defined taking into account system attributes such as:
 - complexity;
 - safety significance;
 - previous experience of similar systems;
 - standardization of design features.
- Sufficient evidence of design, installation, verification and validation activities should be available prior to the assessment. The availability of sufficient evidence could itself be an assessment criterion. The evidence should represent the current/approved state of system design or installation.
- The independence of the assessor(s) must be appropriate.
- The assessor(s) should have experience and knowledge appropriate to the technology and application area of the system being assessed.
- A systematic and consistent approach to FSA should be maintained throughout the lifecycle and across systems. FSA is a subjective activity therefore detailed guidance, possibly through the use of checklists, as to what is acceptable for an organisation should be defined to remove as much subjectivity as possible.

Records generated from the FSA should be complete and the conclusions agreed with those responsible for the management of functional safety for the SIS prior to commencement of the next lifecycle phase.

5.2.6.1.2 The need for someone independent to the project team is to increase objectivity in the assessment. The need for someone of senior stature (for example, experience, grade level, position) is to ensure their concerns are duly noted and addressed. As the note also suggests, on some large projects or assessment teams, it may be necessary to have more than one senior person on this team that is independent to the original project team.

Depending upon the company organisation and expertise within the company, the requirement for an independent assessor may have to be met by using an external organisation. Conversely, companies that have internal organisations skilled in risk assessment and the application of safety instrumented systems, which are independent to and separate (by ways of management and other resources) from those responsible for the project, may be able to use their own resources to meet the requirements for an independent organisation.

5.2.6.1.3 The amount of assessment depends on the size and complexity of a project. It may be possible to assess the results of different phases at the same time. This is particularly true in the case of small changes in a running plant.

5.2.6.1.4 In some countries, a functional safety assessment undertaken at stage 3 is often referred to as the Pre-Startup-Safety-Review (PSSR).

5.2.6.1.5 No further guidance provided.

5.2.6.1.6 No further guidance provided.

5.2.6.1.7 The assessment team should have access to any information they deem necessary for them to conduct the assessment. This should include information from the hazard and risk assessment, design phase through installation, commissioning and validation.

5.2.6.2 Auditing and revision

5.2.6.2.1 This subclause is intended to give guidance about auditing, using an example illustrating relevant activities.

a) Audit categories

Safety instrumented system audits provide beneficial information to plant management, instrument maintenance engineers and instrument design engineers. This enables management to be proactive and aware of the degree of implementation and effectiveness of their safety instrumented systems. Many types of audits, which can be carried out exist. The actual type, scope, and frequency of the audit of any specific activity should reflect the potential impact of the activity on the safety integrity.

Types of audit include:

- 1) audits, both independent and self-audit;
- 2) inspections;
- 3) safety visits (for example, plant walk about and incident review);
- 4) safety instrumented systems surveys (via questionnaires).

A distinction needs to be made between “surveillance and checking” and audit activities. Surveillance and checking focuses on evaluating the performance of specific lifecycle activities (for example, supervisor checking completion of maintenance activity prior to the component being returned to service.) In contrast, audit activities are more comprehensive and focus on overall implementation of safety instrumented systems concerning the safety lifecycle. An audit would include determination as to whether the surveillance and checking program is carried out.

Audits and inspections may be carried out by a company's/site's/plant's/project's own staff (for example, self-audit) or by independent persons (for example, corporate auditors, quality assurance department, regulators, customers or third parties).

Management at the various levels may want to apply the relevant type of audit to gain information on the effectiveness of the implementation of their safety instrumented systems. Information from audits could be used to identify the procedures that have not been properly applied, leading to improved implementation.

b) Audit strategy

Site/plant/project implementing audit programmes might consider rolling, independent or self-audit and inspection programmes.

Rolling programmes are updated regularly to reflect previous safety instrumented systems performance and audit results, and current concerns and priorities. These cover all site/plant/project related activities and aspects of the safety instrumented systems in an appropriate time period and to an appropriate depth.

The primary reason for, and the added value from audits comes from acting on the information they provide in a timely manner. The actions aim to strengthen the effectiveness of safety instrumented systems, for example, to help minimize the risk of employees or members of the public being injured or killed, contribute to improving safety culture, contribute to prevent any avoidable release of substance into the environment.

In summary, the audit strategy may have a mix of audits types, driven by management (the customer), and in order to feed back the relevant information up the management chain for timely action.

c) Audit process and protocols

The overall aim is to achieve maximum value from the performance of the audit, which can only be achieved when all parties (including auditors, contact nominee, plant managers and head of departments, etc.) understand the need for and can influence each audit. The following audit process and protocols might help to ensure some consistency in the approach to achieving these aims. They bear on the following five key stages of the audit process:

1) Audit strategy and programme

The purpose of each audit should be clearly defined and the audit groups identified, together with the roles and responsibilities of each audit group.

There should be an auditing strategy.

There should be a programme of audits.

There should be regular reviews of the audit process, programme and strategy implementation.

2) Audit preparation and pre-planning

Prior to commencement of an audit, the senior manager of the site/plant/project and/or the appropriate audit coordinator should identify a contact nominee.

The auditors and contact nominee should at an early stage discuss, understand and agree on:

- the scope of the audit;
- the timing of the audit;
- the people who need to be available;
- the basis for the audit or audit standard;
- putting the extra effort into the preparation stage and involving the plant personnel, thereby increasing the chances of a successful audit.

The following should be used as a guide for time to be spent at each stage:

- audit preparation: 30 %
- conducting the audit: 40 %
- reporting of findings: 20 %
- audit follow-up: 10 %

The auditor should prepare for the audit by gathering information, procedures/instructions etc., and data and preparing checklists when appropriate.

The auditor should highlight and explain how the possibility of a change to the scope of the audit may occur during the audit, if serious observations/failings are discovered.

3) Conducting the audit

The auditor is to conduct the audit within groups of consecutive days during the set audit period, taking due cognisance of possible disruption to site/plant/project personnel.

The contact nominee should be periodically briefed during the audit of the findings identified, thereby avoiding surprises at the end of the audit.

The auditor should try to involve plant personnel in the audit process in order to impart learning and understanding (of the process and findings) to achieve ownership.

The style of the auditor is crucial to the success of the audit – he should try to be helpful, constructive, courteous, focused and objective.

As a minimum the auditor should try to achieve the agreed scope and timetable - variations will need to be negotiated.

4) Reporting the findings

The auditor should hold a closing meeting either at the end of the audit or later, but before the final report is issued.

The appropriate management should be given the opportunity to comment on the draft report and findings and discuss these at a formal close out meeting if desired.

It is normal practice to request a plan of action from the site/plant/project to address the findings of the report.

5) Audit follow-up

Audit reports normally require a response in the form of an action plan. The auditor might verify satisfactory completion of the action at the due date or at the next audit, whichever is appropriate.

Site/plant/project tracking systems may be used to check the implementation of action plans.

A periodic review/summary of audit findings of each audit group should be considered and its results widely communicated.

The findings/outcome from audits may be used to review the frequency of audits and are input to the management review of safety instrumented systems.

5.2.6.2.2 This subclause reinforces the role that management of change plays in the auditing process.

5.2.7 SIS configuration management

5.2.7.1 Requirements

5.2.7.1.1 To manage and maintain traceability of devices through the lifecycle, a mechanism to identify, control and track the model/versions of each device may be established.

At the earliest possible stage of the safety lifecycle, a unique plant identification should be given to each device. In some cases, earlier models/versions still in use may also be maintained and controlled. This is the first step in the configuration management program which should incorporate the following considerations.

The configuration management system may include:

- a) the provision of a procedure for identification of all devices during all phases of the lifecycle;
- b) the unique identification, of the model/version and build status of each device including software, including the supplier, date and where applicable, change from the model/version originally specified;
- c) the identification and tracking of all actions and changes resulting from fault observations and audits;
- d) control of the issue of a release into service, identifying the status and model/version of the associated devices;
- e) safeguards that have been established to assure that unauthorised alterations/modifications are not made to the SIS while in operation;
- f) the identification of the versions of each software item which together constitute a specific version of a complete device;
- g) the provision of co-ordination for the updating of multiple SIS in one or more plants;
- h) documented authorisation of release into service;
- i) an authorised list of signatures for device release into service;
- j) the stage/phase devices are brought under configuration control;
- k) control of the associated deliverable documentation;
- l) identification of the each model/version of a device;
 - functional specification;
 - technical specification;
- m) all departments/organizations involved in the management and maintenance of SIS are identified and responsibilities assigned and understood.

6 Safety lifecycle requirements

6.1 Objectives

The functional safety achieved in any process facility is dependent on a number of activities being carried out in a satisfactory manner. The purpose of adopting a systematic safety lifecycle approach towards a safety instrumented system is to ensure that all the activities necessary to achieve functional safety are carried out and that it can be demonstrated to others that they have been carried out in an appropriate order. IEC 61511-1 sets out a typical lifecycle in Figure 8 and Table 2. Requirements for each lifecycle phase are given in Clauses 8 through 16 of IEC 61511-1.

The standard recognizes that the specified activities might be structured in different ways, provided that all the requirements are complied with. This restructuring can be beneficial if it allows safety activities to be better integrated into normal project procedures. The purpose of Clause 6 of IEC 61511-1 is to ensure that if a different safety lifecycle is used, the inputs and output of each phase of the lifecycle are defined and all essential requirements are incorporated.

6.2 Requirements

6.2.1 The key consideration is to define in advance the safety lifecycle of the SIS that is going to be used. Experience has shown that problems are likely to occur, unless this activity is planned well in advance and agreements are reached with all persons, departments and organizations taking responsibility. At best, some work will be delayed or have to be redone; at worst, safety can be compromised.

6.2.2 Although it is not a requirement, it is generally beneficial at an early stage to map the proposed safety lifecycle of the SIS on to the project lifecycle of the process including which of the boxes in IEC 61511-1 Figure 8 apply to the project. When doing this, the information needed to begin a safety lifecycle activity should be considered together with who is likely to be able to provide it. In some cases it may not be possible to determine accurate information on a particular issue until late in the design phase. In such cases, it may be necessary to make an estimate based on previous experience and then confirm the data at a later date. Where this is the case, it is important to note this on the safety lifecycle.

6.2.3 Another important part of safety lifecycle planning is to identify the techniques that will be used during each phase. The identification of such techniques is important since it is often necessary to use a specific technique that requires persons or departments with unique skills and experiences. For instance, consequences in a particular application may be dependent on the maximum pressure developed after a failure event; and the only way this can be determined is to develop a dynamic model of the process. The information requirements for dynamic modelling will then have an important impact on the design process.

7 Verification

7.1 Objective

The purpose of verification is to ensure that the activities for each safety lifecycle phase, as determined by verification planning, have, in fact, been carried out and that the required outputs of the phase, whether they be in the form of documentation, hardware or software, have been produced and are suitable for their purpose.

7.1.1 Requirements

7.1.1.1 IEC 61511-1 recognizes that organizations will have their own procedures for verification and do not always require them to be carried out in the same way. Instead, the intent of this subclause is that all verification activities are planned in advance, along with any procedures, measures and techniques that are to be used.

7.1.1.2 No further guidance provided.

7.1.1.3 It is important that the results of verification are available so that it can be demonstrated that effective verification has taken place at all phases of the safety lifecycle.

8 Process hazard and risk assessment

8.1 Objectives

The overall objective here is to establish the need for safety functions (for example, protection layers) together with associated levels of performance (risk reduction) that are needed to ensure a safe process. It is normal in the process sector to have multiple safety layers so that failure of a single layer will not lead to or allow a harmful consequence. Typical safety layers are represented in Figure 9 of IEC 61511-1.

8.2 Requirements

8.2.1 The requirements for hazard and risk assessment are specified only in terms of the results of the task. This means that an organization may use any technique that it considers to be effective, provided it results in a clear description of safety functions and associated levels of performance.

A hazard and risk assessment should identify and address the hazards and hazardous events that could occur under all reasonably foreseeable circumstances (including fault conditions and reasonably foreseeable misuse).

On a typical project in the process sector, a preliminary hazard and risk assessment needs to be carried out early during the basic process design. An assumption at this stage is that hazards have been eliminated or reduced as far as is reasonably practicable, by the application of inherent safety principles and the application of good engineering practice (this activity of hazard reduction is not within the scope of IEC 61511). For the SIS, this preliminary hazard and risk assessment is important because establishing, designing and implementing an SIS are complex tasks and can take a considerable length of time. Another reason for undertaking this work early is that information on system architecture will be needed before the process and instrumentation diagrams are finalized. There will usually be sufficient information enabling preliminary hazard and risk assessment to proceed once a process flow diagram has been completed and all of the initial process data is available. It should be recognised that additional hazards may be introduced as detailed design proceeds. A final hazard and risk assessment may therefore be necessary once the process and instrumentation diagram has been finalized. This final analysis generally uses a formal and fully documented procedure such as hazard and operability study (HAZOP). It should confirm that the safety layers as designed are adequate to ensure the safety of the plant. During this final analysis it is necessary to consider whether failures in the safety systems introduce any new hazards or demands. If any new hazards are established at this stage, it may be necessary to define new safety functions. Another more likely outcome is that additional events are identified that lead to the hazards that were already identified at the preliminary stage. It will then be necessary to consider if any revision of the safety functions and performance requirements that were determined in the original analysis is needed.

The approach used to identify hazards will depend on the application being considered. For certain simple processes where there is extensive operating experience of a standard design, such as simple off-shore wellhead towers, it may be sufficient to use industry developed check lists (for example, the safety analysis checklists in ISO 10418 and API RP 14C).

Where the design is more complex or a new process is being considered, a more structured approach may be necessary (for example, IEC 60300-3-9:1995).

NOTE Further information on selection of appropriate techniques is given in ISO 17776.

When considering the consequences of a particular failure event, all possible outcomes, and the frequency of the failure event as it contributes to each outcome, should be analysed. No credible outcome should be ignored or discarded from a risk analysis. Exposing piping or vessels to pressures above design will not always result in catastrophic loss of containment. In many cases, equipment will have been subjected to test pressure greater than design and the only consequence may be leakage of flammable substances leading to the possibility of fire. In evaluating consequences, persons responsible for the mechanical integrity of the plant will need to be consulted. They will need to take into account the original test pressure but also whether the original design included corrosion allowances and whether a corrosion management programme is in place. Where consequences are based on such assumptions, it is important that this is clearly stated so that relevant procedures can be incorporated into the safety management system. A further issue when considering consequences will be the number of persons likely to be effected by a particular hazard. In many cases, operational and maintenance staff will only be present in the hazardous zone on an infrequent basis and this should be taken into account when predicting consequences. Care is needed when using this statistical approach since it will not be valid in all cases, such as where the hazard only occurs during start-up and staff are always present. Also considerations should be given to the potential increased number of people being in the vicinity of the hazardous event as a result of investigating the symptoms during the build-up to the event.

When assessing the potential sources of demand on the SIS, the assessment should include the following situations: start-up, continuous operation, shutdown, maintenance errors, manual interventions (for example, controllers on manual) loss of services (for example, air, cooling water, nitrogen, power, steam, trace heating, etc.).

When considering the frequency of demands, it may be necessary in some complex cases to undertake a fault tree analysis. This is often necessary where severe consequences only result from simultaneous failure of more than one event (for example, where relief headers are not designed for worst case relief from all sources). Judgement will need to be made on when operator errors are to be included in the list of events that can cause the hazard and the frequency to be used for such events. Operator error could often be excluded if the action is subject to permit procedures or lock-off facilities are provided to prevent inadvertent action. Care is also needed where credit is taken for reduction in demand frequency due to operator action. The credit that can be taken will need to be limited by human factor issues such as how quickly action needs to be taken and the complexity of the tasks involved. Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10, then the overall system will need to be designed according to IEC 61511-1. The system that undertakes the safety function would then comprise the sensor detecting the hazardous condition, the alarm presentation, the human response and the equipment used by the operator to terminate any hazard. It should be noted that a risk reduction of up to a factor of 10 might be claimed without the need to comply with IEC 61511. Where such claims are made, the human factor issues will need to be carefully considered. Any claims for risk reduction from an alarm should be supported by a documented description of the necessary response for the alarm and that there is sufficient time for the operator to take the corrective action and assurance that the operator will be trained to take the preventive actions.

An alarm system can be used as a method of risk reduction by reducing the demand rate on the SIS providing:

- the sensor used for the alarm system is not used for control purposes where loss of control would lead to a demand on the SIS;
- the sensor used for the alarm system is not used as part of the SIS;
- limitations have been taken into account with respect to risk reduction that can be claimed for the BPCS and common cause issues.

Examples of techniques that can be used to establish the SIL of safety instrumented systems are given in IEC 61511-3 which also contains guidance on what to consider when selecting the method to use for a specific application.

When establishing whether risk reduction is required it is necessary to have some process safety and environmental targets. These may be specific to the particular site or operating company and will be compared with the level of risk without additional safety functions. After establishing the need for risk reduction, it will be necessary to consider what functions are required to be carried out to return the process to a safe state. In theory, the functions may be described in general terms without a reference to a particular technology. In the case of over-pressure protection for instance, the function may be described as prevention of pressure rise above a specified value. Either a relief valve or a safety instrumented system could then carry out this function. If the function is described as above, the selection of the type of technology to use would be decided in the next lifecycle step (allocation of safety instrumented functions to protection layers). In practice, the functional requirements would be different depending on the type of system selected; and this stage, and the next, may in some cases be combined.

In summary, the hazard and risk analysis should consider the following:

- each determined hazardous event and the event sequences that contribute to it;
- the consequences and likelihood of the event sequences with which each hazardous event is associated; these may be expressed quantitatively or qualitatively;
- the necessary risk reduction for each hazardous event;
- the measures taken to reduce or remove hazards and risks;
- the assumptions made during the analysis of the risks, including the estimated demand rates and equipment failure rates; any credit taken for operational constraints or human intervention should be detailed;
- references to key information which relates to the safety-related systems at each SIS lifecycle phase (for example verification and validation activities).

The information and results which constitute the hazard and risk analysis should be documented.

It may be necessary for the hazard and risk assessment to be repeated at different stages in the overall SIS safety lifecycle, as decisions are taken and available information becomes more refined.

8.2.2 In the process industry, an important cause of demands that will need to be considered in many applications is the BPCS failure. It should be noted that failure of the BPCS may be caused by the sensor, valve or control system.

Sometimes, control systems used in the process industry have redundant processors but sensors and valves are usually non-redundant. When assigning a failure rate to the BPCS, there is an important limitation that needs to be recognised. IEC 61511-1 limits the dangerous failure rate, in relation to a particular hazard, that can be claimed to 10^{-5} per hour unless the system is implemented according to the requirements of this standard. The reason for the limit is that if a lower dangerous failure rate is claimed, it would be in the range of failure rates within Table 4 of IEC 61511-1. The limit ensures that high levels of confidence are not placed on systems that do not meet the requirements of IEC 61511-1.

8.2.3 No further guidance provided.

9 Allocation of safety functions to protection layers

9.1 Objective

In order to determine the need for a SIS and its associated SIL, it is important to consider what other protection layers exist (or need to exist) and how much protection they provide. After considering the other protection layers, a determination should then be made on the need for a SIS protection layer. If a SIS protection layer is needed, a determination should then be made on the SIL for the safety instrumented function(s) of this SIS.

9.2 Requirements of the allocation process

9.2.1 The requirement here is to agree on the safety layers to be used and to allocate performance targets for the safety instrumented functions. In practice, safety functions are in many cases only allocated to safety instrumented systems where there are problems in using inherently safe designs or other technology systems.

Examples of such problems include limitations on flare capacity or protection against exothermic reactions. Any decision to use instrument based systems rather than more traditional approaches such as relief valves will need to be supported by sound reasons that will stand up to regulatory authority challenge.

As stated above, the hazard and risk assessment and allocation may be concurrent activities or allocation may in some circumstances take place prior to hazard and risk assessment. Decisions on the allocation of safety functions to safety layers are often taken on the basis of what has been found to be practicable by the user organization. Established industry good practice should also be taken into account. Decisions will then be taken on the safety instrumented systems, assuming credit for the other safety layers. For example, where relief valves have been installed and these have been designed and installed according to industry codes, it may then be decided that these are adequate on their own to achieve adequate risk reduction. Safety instrumented systems would then only limit pressure where size or performance of the relief valve(s) was insufficient for the application or release to the atmosphere is to be prevented.

9.2.2 No further guidance provided.

9.2.3 When a safety function is allocated to a safety instrumented function, it will be necessary to consider whether the application is in demand or in continuous mode. The majority of applications in the process sector operate in demand mode where demands are infrequent. In such cases, Table 3 in IEC 61511-1 is the appropriate measure to use. There are some applications where demands are frequent (for example, greater than one per year) and it is more appropriate to consider the application as continuous mode because the probability of dangerous failure will be primarily determined by the failure rate of the SIS. In such cases, Table 4 in IEC 61511-1 is the appropriate measure to apply. Continuous mode applications where failure would result in an immediate hazard are rare. Burner or turbine speed control may be continuous mode applications if protection systems are insufficient for all failure modes of the control system.

Table 3 of IEC 61511-1 defines SIL in terms of PFD_{avg} . The target PFD_{avg} will be determined by the required risk reduction. The required risk reduction can be determined by comparing the process risk without the SIS with the tolerable risk. This can be determined on a quantitative or qualitative basis using the techniques in IEC 61511-3.

Table 4 of IEC 61511-1 defines SIL in terms of the target frequency of dangerous failures to perform the SIF. This will be determined by the tolerable failure rate of the SIS, taking into account the consequence of failure in a particular application. When Table 4 of IEC 61511-1 is used to determine the required SIL, the target is based on the frequency of dangerous failure for the safety instrumented system. In using Table 4 of IEC 61511-1, it is incorrect to convert the frequency of dangerous failure into a probability of dangerous failure on demand using the proof test interval or the demand rate. While the units may appear to be correct, this results in an inappropriate conversion of Table 4 of IEC 61511-1 and may result in under-specification of the safety function SIL requirements.

The targets for average probability of failure on demand or frequency of dangerous failures per hour apply to the safety instrumented function, not to individual components or subsystems. A component or subsystem (for example, sensor, logic solver, final element) cannot have a SIL assigned to it outside its use in a specific SIF. However, it can have an independent maximum SIL capability claim.

The outcome of the hazard and risk assessment and allocation process should be a clear description of the functions to be carried out by the safety systems, including potential safety instrumented systems together with safety integrity level requirements (along with mode of operation, continuous or demand) for any safety instrumented function. This forms the basis for the SIS safety requirements specification. The description of the functions should be clear as to what needs to be done to ensure that safety is maintained.

At this stage of the implementation, it is unnecessary to specify architectural details for sensors and valves. Decisions on architectures are complex and whether a particular system requires 2oo3 sensors and 1oo2 valves will depend on many factors.

9.2.4 The implications of Tables 3 and 4 of IEC 61511-1 need to be fully understood. In particular, the PFD_{avg} that can be claimed for a single safety instrumented function is limited to 10^{-5} , corresponding to a risk reduction of 10^5 (SIL 4). Reliability analysis may indicate that it is possible to achieve a PFD_{avg} due to random hardware failures of less than 10^{-5} , but IEC 61511-1 presumes that systematic failures and common mode failures will limit the actual performance that can be achieved. It is strongly recommended that where risk analysis shows such a high risk reduction to be necessary, the difficulty of achieving a SIL 4 safety instrumented function in the process sector should be noted. Consideration should be given to using multiple independent SISs, of lower integrity.

With reference to Note 4:

Multiple SISs may be utilized in order to achieve higher levels of risk reduction (for example, greater than 10^3). When using multiple SISs to achieve higher risk reduction, it is important that each of the SISs is independently able to carry out the safety function and that there is sufficient independence between the SISs. For example, it might not be advisable to combine a SIL 2 pressure sensing loop with a SIL 1 level sensing loop to achieve an over pressure safety function having a risk reduction requirement of 10^3 because by the time the level sensor detected a high level, the vessel might have already exceeded its pressure constraints.

Furthermore, where multiple SISs are used, one should take into account common cause failures. In addition, all of the other requirements defined in IEC 61511-1 should be satisfied, including the minimum fault tolerance requirements defined in Table 5.

To illustrate how combining multiple SISs might be used to achieve higher levels of risk reduction, consider the following example:

A 2oo3 transmitter set, a 2oo3 logic solver and a 1oo2 final element set which yields a SIS with a PFD_{avg} of $3,05 \times 10^{-4}$. This SIS achieves a risk reduction of approx. $3,3 \times 10^3$.

It would be incorrect to assume that using two such systems together would result in a risk reduction of 10×10^6 ($3,3 \times 10^3 \times 3,3 \times 10^3$). Common cause factors, such as using similar technologies, designing both systems from the same functional specification, human factors (for example, programming, installation, maintenance), external factors (for example, corrosion, plugging, freezing of air lines, lightning) will limit the system improvement. It would also be necessary to take into account any components shared between the two systems.

A more feasible solution may be to utilize a non-redundant second system using components as diverse as possible (in order to minimize potential common cause problems).

For example consider a SIS comprising a single switch, relay logic and a single final element which yields a system with a PFD_{avg} of $7,7 \times 10^{-3}$. This system achieves a risk reduction of approx. $1,3 \times 10^2$.

Combining the software based SIS with the simplex relay SIS results in an overall theoretical risk reduction of $4,3 \times 10^5$ ($3,3 \times 10^3 \times 1,3 \times 10^2$). While combining the performance as shown above appears to be theoretically possible (since either SIS could shut the process unit down), once again, common cause factors have to be taken into account, and the achieved risk reduction will be somewhat less due to these factors.

9.3 Additional requirements for safety integrity level 4

9.3.1 No further guidance provided.

9.3.2 No further guidance provided.

9.4 Requirement on the basic process control system as a layer of protection

9.4.1 The basic process control system may be identified as a protection layer subject to certain conditions. If functions are implemented in the BPCS for the purpose of reducing the process risk, the BPCS can be allocated a risk reduction for the identified risks it is intended to reduce.

9.4.2 Risk reduction of less than 10 may be claimed from instrumented systems without the need to comply with IEC 61511-1. This allows the BPCS to be used for some risk reduction without the need to implement such systems to the requirements of IEC 61511-1. Any claim made should be justified by consideration of the integrity of the BPCS (determined by reliability analysis or performance data) and the procedures used for configuration, modification and operation and maintenance. When allocating risk reduction to functions in the BPCS, it is important to ensure that access security and change management are provided. The risk reduction that can be claimed for a BPCS function is also determined by the degree of independence between the BPCS function and the initiating cause. Figure 2 illustrates independence of the BPCS function and the initiating cause.

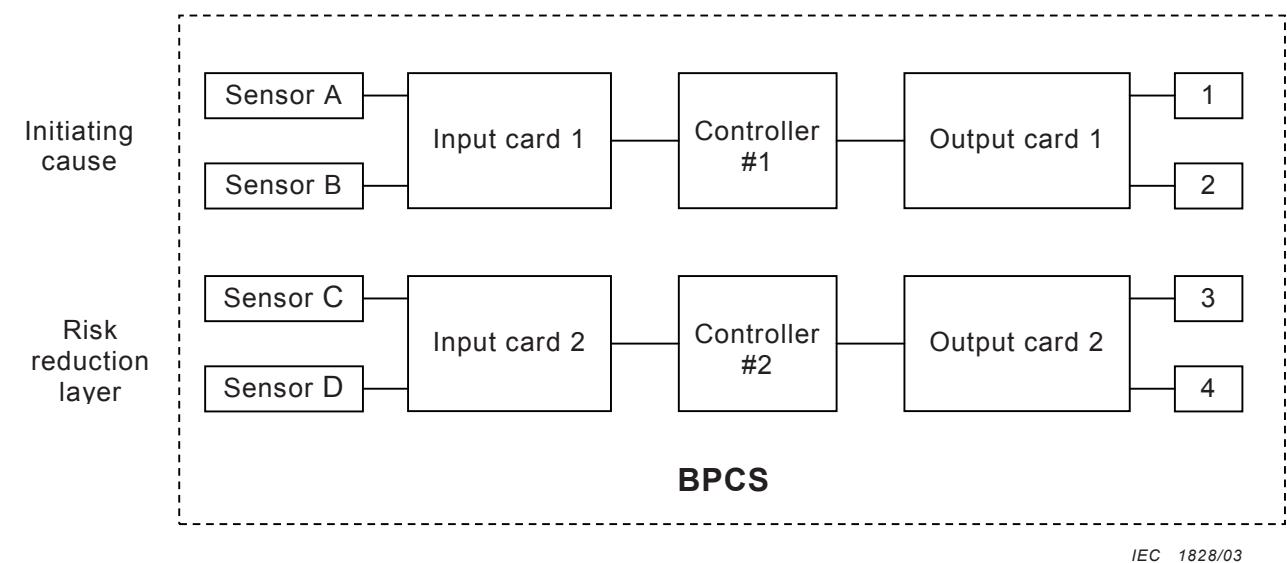


Figure 2 – BPCS function and initiating cause independence illustration

For example, consider the case where a flow control loop is the initiating cause. This initiating cause includes a flow transmitter, a controller, and a control valve. In order to allocate risk reduction to a pressure control loop in the BPCS, the pressure transmitter should be wired to an independent controller, modulating an independent final element (for example, vent valve to flare system).

9.4.3 No further guidance provided.

9.5 Requirements for preventing common cause, common mode and dependent failures

9.5.1 An important issue to be considered at an early stage is whether there are any common cause failures between redundant parts within each layer (for example, between 2 pressure relief valves on the same vessel), between safety layers or between safety layers and the BPCS. An example of this could be where failure of a basic process control system measurement could cause a demand on the safety instrumented system and a device with the same characteristics is used within the safety instrumented system. In such cases it will be necessary to establish if there are credible failure modes that could cause failure of both devices at the same time. Where a common cause of failure is identified then the following actions can be taken.

- a) The common cause can be reduced by changing the design of the safety instrumented system or the basic process control system. Diversity of design and physical separation are two effective methods of reducing the likelihood of common cause failures. This is usually the preferred approach.
- b) The likelihood of the common cause event should be taken into account when determining whether the overall risk reduction is adequate. This may require a fault tree analysis to be constructed that includes demand causes as well as protection system failures. Common cause failures can be represented on such fault trees and their effect on overall risk can be quantified through appropriate modelling methods.

It should be noted that any sensors or actuators which are shared by the BPCS and SIS are very likely to introduce common cause failures and that the approach to such sharing of devices should be as discussed in this **subclause**.

9.5.2 The considerations listed below apply when an assessment is carried out on the likelihood of common cause, common mode and dependent failures. The extent, formality and depth of the assessment will depend on the safety integrity level of the intended function. The effect of common cause, common mode and dependent failures may be dominant for safety integrity levels of 3 or higher. The following should be considered:

- independence between protection layers – a failure mode effects analysis should be carried out to establish if a single event can cause failure of more than one protection layer or failure of the BPCS and a protection layer. The depth and rigor of the analysis will depend on the risk.
- diversity between protection layers - the aim should be diversity between protection layers and the BPCS but this is not always achievable. An example could be over pressure protection where a failure of the BPCS pressure control loop would cause a demand. The BPCS and the SIS will both require pressure measurement and there will be a limit on the suitable equipment available. Some diversity can be achieved by using equipment from different manufacturers but if SIS and BPCS sensors are connected to the process using the same type of hook up, then the diversity may be of limited value.
- physical separation between different protection layers – physical separation will reduce the impact of common cause failures due to physical causes. Measurement connection locations for BPCS and SIS should be given maximum physical separation subject to functional needs such as accuracy and response time.