NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61511-2

Première édition
First edition
2003-07

**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**

**Functional safety –
Safety instrumented systems
for the process industry sector –**

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

Numéro de référence
Reference number
CEI/IEC 61511-2:2004

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (http://www.iec.ch/searchpub/cur_fut.htm) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (http://www.iec.ch/online_news/justpub/jp_entry.htm) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (http://www.iec.ch/searchpub/cur_fut.htm) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (http://www.iec.ch/online_news/justpub/jp_entry.htm) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61511-2

Première édition
First edition
2003-07

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

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

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

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XC

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés «Publication(s) de la CEI»). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61511-2 a été préparée par le sous-comité 65A: Aspects systèmes, du Comité d'Etudes 65 de la CEI: Mesure et commande dans les processus industriels.

Cette version bilingue (2004-07) remplace la version monolingue anglaise.

Le texte anglais de cette norme est issu des documents 65A/387A/FDIS et 65A/390/RVD. Le rapport de vote 65A/390/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

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

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-2 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

This bilingual version (2004-07) replaces the English version.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/387A/FDIS	65A/390/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

The French version of this standard has not been voted upon.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

La CEI 61511 comprend les parties suivantes, sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation* (voir la Figure 1).

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

Partie 2: Lignes directrices pour l'application de la CEI 61511-1

Partie 3: Guide pour la détermination des niveaux d'intégrité de sécurité requis

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 61511 series has been developed as a process sector implementation of IEC 61508 series.

IEC 61511 consists of the following parts, under the general title *Functional safety – Safety Instrumented Systems for the process industry sector* (see Figure 1):

Part 1: Framework, definitions, system, hardware and software requirements

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

Part 3: Guidance for the determination of the required safety integrity levels

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

Les systèmes instrumentés de sécurité sont utilisés depuis des années pour exécuter des fonctions instrumentées liées à la sécurité dans les processus industriels. Si l'instrumentation doit être effectivement utilisée pour réaliser des fonctions instrumentées liées à la sécurité, il est essentiel que cette instrumentation satisfasse à certaines normes.

La présente Norme internationale traite de l'application des systèmes instrumentés de sécurité aux industries de transformation. Elle traite aussi des interfaces entre les systèmes instrumentés de sécurité et les autres systèmes de sécurité, et requiert une évaluation de danger et de risque du processus. Le système instrumenté de sécurité comprend les capteurs, les unités logiques et les éléments terminaux.

Cette Norme internationale traite de deux concepts, qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité et les niveaux d'intégrité de sécurité. Le cycle de vie de sécurité constitue le cadre central qui lie la plupart des concepts de cette Norme internationale.

Les unités logiques du système instrumenté de sécurité mentionnées dans cette norme incluent les technologies électriques (E)/électroniques (E)/et électroniques programmables (PE). Dans le cas où d'autres technologies seraient utilisées pour les unités logiques, les principes fondamentaux de cette norme pourraient également être appliqués. Cette norme concerne également les capteurs et les éléments terminaux des systèmes instrumentés de sécurité, quelle que soit la technologie utilisée. Cette Norme internationale est spécifique de la production industrielle par processus dans le cadre de la série CEI 61508.

La CEI 61511-1 présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Le but de la présente norme est de fournir des lignes directrices sur la façon de satisfaire à la CEI 61511-1.

Pour faciliter l'utilisation de cette norme, les numéros d'articles donnés sont identiques au texte normatif correspondant de la CEI 61511-1 (à l’exception des annexes).

Dans la plupart des cas, la meilleure sécurité est obtenue, chaque fois que cela est possible, par des processus qui soient sûrs de par leur conception même, combinée, au besoin, avec un certain nombre de systèmes de protection, fondés sur différentes technologies [par exemple, chimique, mécanique, hydraulique, pneumatique, électrique, électronique, thermodynamique (par exemple, pare-feu), électronique programmable] couvrant tous les risques résiduels identifiés. Toute stratégie de sécurité prend en compte chacun des systèmes instrumentés de sécurité individuellement, dans le contexte des autres systèmes de protection. Pour faciliter cette approche, cette norme

– requiert une évaluation du danger et du risque pour identifier l'ensemble des prescriptions de sécurité;
– requiert l'allocation des prescriptions de sécurité au(x) système(s) instrumenté(s) de sécurité;
– s'inscrit dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
– détaille l'utilisation de certaines activités, telles que la gestion de la sécurité, qui peuvent être applicables à toute méthode permettant d'obtenir la sécurité fonctionnelle.

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.

Cette Norme internationale sur les systèmes instrumentés de sécurité pour l'industrie de transformation:

– prend en compte les étapes pertinentes du cycle de vie de sécurité, depuis la conceptualisation initiale, en passant par la conception, la mise en oeuvre, l'exploitation et la maintenance, jusqu'au déclassement;

– permet l'harmonisation avec la présente norme des normes spécifiques à l'industrie de transformation, existantes ou de nouveaux pays.

Cette Norme internationale est destinée à conduire à un haut niveau de cohérence (par exemple, pour ce qui est des principes sous-jacents, de la terminologie, des informations) au sein des industries de transformation. Ceci afin d'offrir des améliorations en termes de sécurité et d'économie.

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.

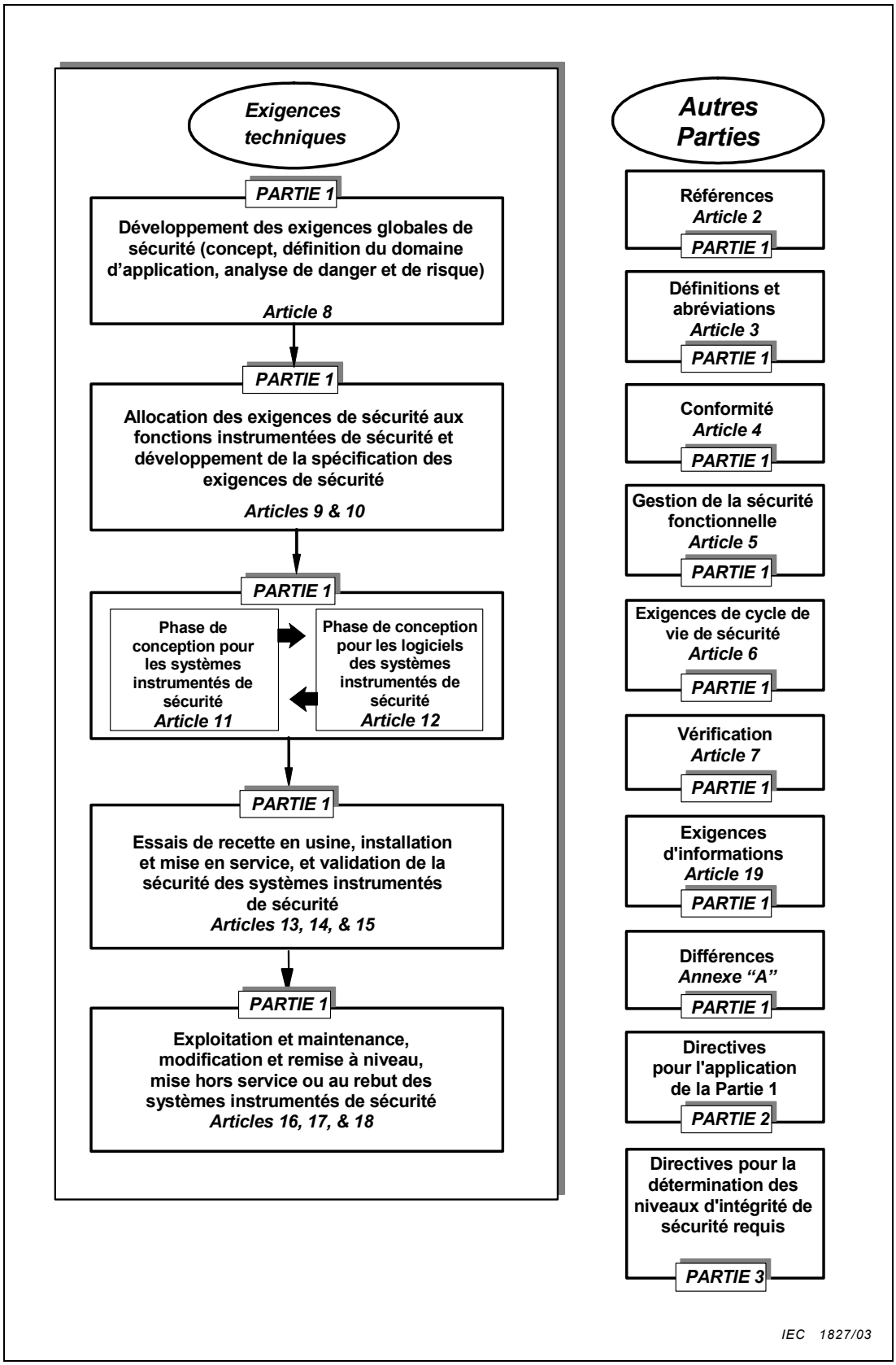


Figure 1 – Structure générale de la présente norme

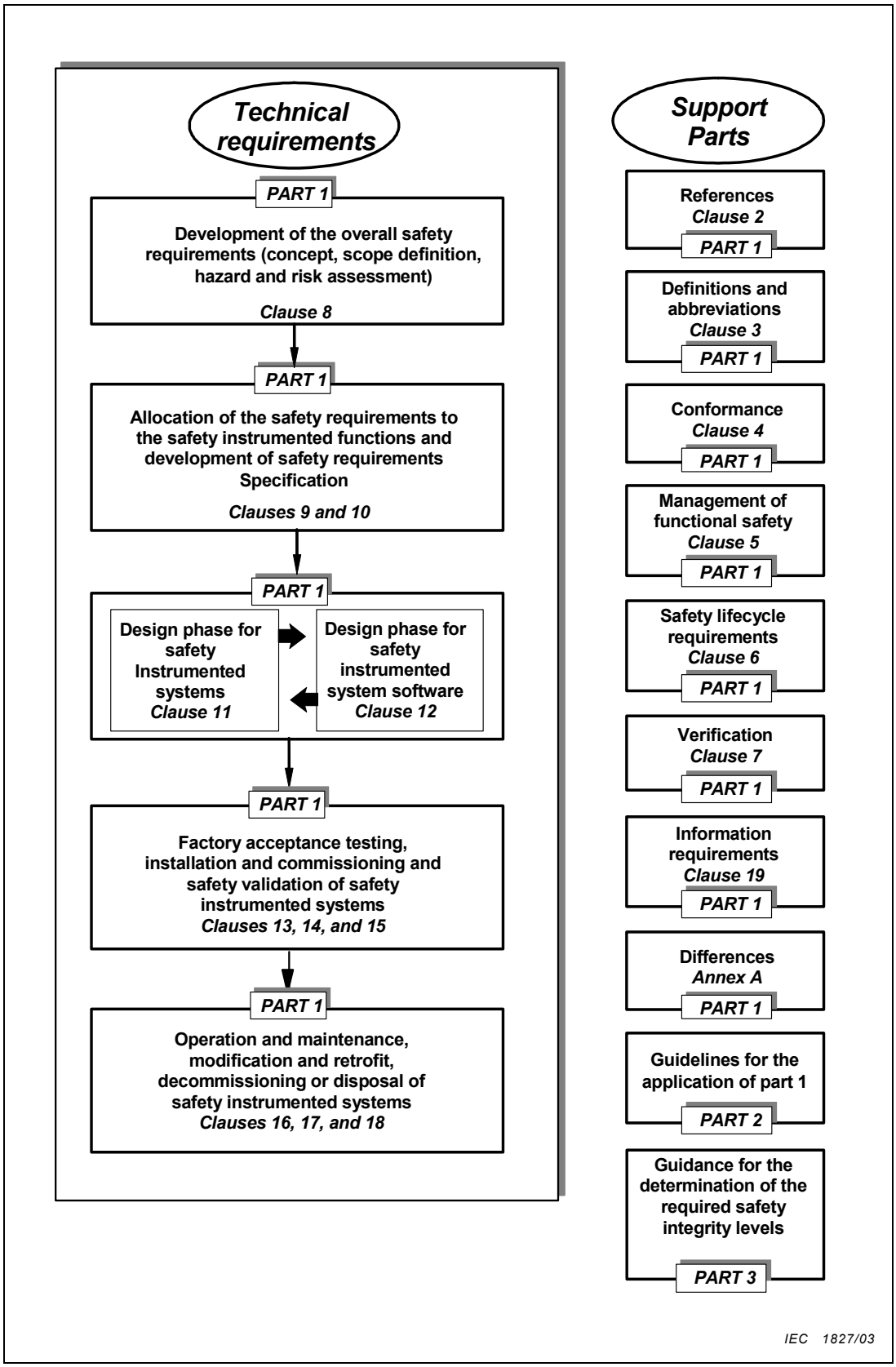


Figure 1 – Overall framework of this standard

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

1 Domaine d'application

La présente Partie 2 de la CEI 61511 donne des conseils sur la spécification, la conception, l'installation, l'exploitation et la maintenance des fonctions instrumentées de sécurité et du système instrumenté de sécurité concerné, comme cela est défini par la CEI 61511-1. La présente Partie 2 de la CEI 61511 a été organisée de sorte que chaque numéro d'article mentionné corresponde au même numéro d'article que celui de la CEI 61511-1 (à l'exception des annexes).

2 Références normatives

Aucune ligne directrice n'est fournie.

3 Termes, définitions et abréviations

Aucune ligne directrice n'est fournie, excepté pour les définitions 3.2.68 et 3.2.71.

3.2.68
fonction de sécurité

Il convient qu'une fonction de sécurité prévienne l'arrivée d'un événement dangereux spécifié. Par exemple, «empêcher que la pression dans le réservoir #ABC456 ne dépasse 100 bars». Une fonction de sécurité peut être obtenue par:

a) un système instrumenté de sécurité unique (SIS), ou

b) un ou plusieurs systèmes instrumentés de sécurité et/ou d'autres couches de protection.

Dans le cas b), chaque système instrumenté de sécurité ou toute autre couche de protection sera capable de réaliser la fonction de sécurité et la combinaison globale permettra d'obtenir la réduction de risque requise (cible de sécurité du processus).

3.2.71
fonction de sécurité

Les fonctions instrumentées de sécurité sont dérivées de la fonction de sécurité, ont un niveau d'intégrité de sécurité (SIL) associé et sont réalisées par un système instrumenté de sécurité (SIS) spécifique. Par exemple, «fermer la vanne #XY123 en 5 s, lorsque la pression dans le réservoir #ABC456 atteint 100 bars». Notez que les composants d'un système instrumenté de sécurité peuvent être utilisés par plusieurs fonctions instrumentées de sécurité.

4 Conformité à cette Norme internationale

Aucune ligne directrice n'est fournie.

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 Gestion de la sécurité fonctionnelle

5.1 Objectif

L'objectif de l'Article 5 de la CEI 61511–1 est de fournir des exigences pour mettre en oeuvre les activités de gestion nécessaires pour garantir que les objectifs fonctionnels de sécurité sont remplis.

5.2 Exigences

5.2.1 Généralités

5.2.1.1 Aucune ligne directrice n'est fournie.

5.2.1.2 Lorsqu'un organisme a la responsabilité d'une ou de plusieurs activités nécessaires à la sécurité fonctionnelle et que cet organisme travaille selon des procédures d'assurance qualité, de nombreuses activités décrites dans cet article seront déjà conduites dans un but de qualité. Lorsque c'est le cas, il se peut qu'il soit inutile de répéter ces activités dans un but de sécurité fonctionnelle. Dans de tels cas, il convient que les procédures d'assurance qualité soient passées en revue pour être sûr qu'elles conviennent, de manière que les objectifs de la sécurité fonctionnelle soient atteints.

5.2.2 Organisation et ressources

5.2.2.1 Il convient que la structure organisationnelle associée aux systèmes instrumentés de sécurité dans une Société/sur un Site/sur une Installation industrielle/pour un Projet soit définie et que les rôles et les responsabilités de chacun soient clairement compris et soient communiqués. Dans la structure, il convient que les différents rôles soient identifiés individuellement, que leurs buts soient précisés et qu'ils soient décrits. Il convient que les responsabilités incombant à chaque rôle soient identifiées très clairement; il convient également que des responsabilités spécifiques soient identifiées. En outre, il convient de définir à qui chaque personne rend compte et de désigner la personne responsable des affectations. Le but est d'assurer que chaque personne, dans une organisation, comprend son rôle et ses responsabilités vis-à-vis des systèmes instrumentés de sécurité.

5.2.2.2 Il convient que les compétences et les connaissances requises pour mettre en oeuvre toute activité du cycle de vie de sécurité relative aux systèmes instrumentés de sécurité soient identifiées; et pour chaque qualification, il convient que les niveaux requis de compétence soient définis. Il convient que les ressources soient évaluées par rapport à chaque qualification vis-à-vis des compétences et également par rapport au nombre de personnes requises par qualification. Lorsque des différences sont identifiées, il convient que des programmes d'aménagement soient établis pour permettre aux niveaux de compétence requis d'être obtenus à temps. En cas de pénurie de compétences, le personnel convenablement qualifié et expérimenté peut être recruté ou employé sous contrat.

5.2.3 Evaluation et gestion des risques

L'exigence indiquée en 5.2.3 de la CEI 61511–1 stipule que les dangers sont identifiés, les risques évalués et que la réduction de risque en découlant nécessairement est déterminée. Il est admis qu'il y a de nombreuses méthodologies différentes et disponibles pour effectuer ces évaluations. La CEI 61511-1 ne privilégie aucune méthodologie particulière. Au contraire, le lecteur est encouragé à passer en revue un certain nombre de méthodologies traitant de cette question dans la CEI 61511-3. Voir 8.2.1 pour d'autres conseils.

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 Planification

Le but de ce paragraphe est de s'assurer que, dans le projet global, une planification adéquate de la sécurité est conduite, de sorte que toutes les activités requises pendant chaque phase du cycle de vie soient traitées (par exemple, conception technique, exploitation en installation industrielle). La norme n'exige aucune structure particulière pour ces activités de planification, mais elle demande la mise à jour ou l'examen périodique de celles-ci.

5.2.5 Mise en oeuvre et surveillance

5.2.5.1 Le but de ce paragraphe est de s'assurer que des procédures efficaces de gestion sont en place pour

– veiller à ce que toutes les recommandations résultant de l'analyse de danger, de l'évaluation de risque, de toute autre évaluation et activité d'audit, de vérification et de validation, aient été prises en compte d'une manière satisfaisante, et pour
– vérifier que le SIS fonctionne bien selon les exigences spécifiées en ce qui concerne la sécurité durant toute sa vie opérationnelle.

5.2.5.2 Il est à noter que, dans ce contexte, les fournisseurs pourraient inclure des entreprises de conception et des entreprises de maintenance, ainsi que des fournisseurs de composants.

5.2.5.3 Il convient qu'un examen des performances du SIS soit périodiquement entrepris pour s'assurer que les hypothèses d'origine, faites pendant le développement de la spécification des exigences concernant la sécurité (SRS), continuent d'être respectées. Par exemple, il convient qu'un examen périodique du taux de défaillance estimé de différents composants dans un SIS soit effectué, pour s'assurer qu'il demeure tel qu'il a été défini à l'origine. Si les taux de défaillance sont plus mauvais que ceux prévus à l'origine, une modification de la conception peut être nécessaire. De même, il convient que le taux de sollicitation sur le SIS soit examiné. Si le taux est plus élevé que celui qui a été estimé à l'origine, un ajustement du niveau d'intégrité de sécurité (SIL) peut alors être nécessaire.

5.2.6 Evaluation, audits et révisions

Les évaluations et les audits sont des outils destinés à la détection et à l'élimination des erreurs. Les alinéas ci-dessous font clairement la distinction entre ces activités.

L'évaluation fonctionnelle de la sécurité vise à évaluer si les dispositions prises pendant les phases du cycle de vie qui sont prévues sont adéquates pour la réalisation de la sécurité ou non. Les décisions finales sont prises par des examinateurs sur la base des décisions prises par les responsables de la réalisation de la sécurité fonctionnelle. Il s'agit, par exemple, de procéder à une évaluation avant la mise en service, afin de déterminer si les procédures de maintenance sont adéquates ou non.

Les auditeurs de la sécurité fonctionnelle détermineront à partir des dossiers du projet ou de l'installation industrielle si les procédures nécessaires ont été appliquées ou non, à la fréquence spécifiée, par des personnes ayant la compétence nécessaire. Il n'est pas demandé aux auditeurs de porter des jugements sur l'adéquation du travail qu'ils sont en train d'étudier. Si toutefois ils se rendent compte qu'il peut être bénéfique de faire des modifications, il convient alors qu'une observation soit incluse dans le rapport.

Il convient de noter que dans de nombreux cas il peut y avoir une superposition du travail de l'examinateur et de l'auditeur. Par exemple, un auditeur peut devoir déterminer non seulement si un opérateur a reçu la formation nécessaire, mais en plus porter un jugement quant à savoir si la formation a eu comme résultat l'obtention de la compétence requise.

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 Evaluation de la sécurité fonctionnelle

5.2.6.1.1 L'utilisation de l'évaluation de la sécurité fonctionnelle (FSA) est fondamentale pour démontrer qu'un système instrumenté de sécurité (SIS) remplit ses exigences concernant la (les) fonction(s) instrumentée(s) de sécurité et le niveau d'intégrité de sécurité (SIL). L'objectif de base de cette évaluation est de démontrer la conformité aux normes et aux pratiques agréées, par l'intermédiaire d'une évaluation indépendante du processus de développement du système. Une évaluation d'un SIS peut être nécessaire à différentes étapes du cycle de vie. Afin de conduire une évaluation efficace, il convient de développer une procédure qui définit le domaine d'application de cette évaluation, ainsi que quelques indications sur le profil de l'équipe d'évaluation.

Les attributs suivants sont considérés comme étant de bonne pratique pour l'évaluation de la sécurité fonctionnelle.

- Il convient qu'un plan soit établi pour chaque FSA, identifiant les dispositions tels que le domaine d'application de l'évaluation, les examinateurs, les compétences des examinateurs et les informations à générer par l'évaluation.
- Il convient que la FSA prenne en compte d'autres normes et usages, qui peuvent être contenus dans des normes externes ou internes à l'entreprise, des guides, des procédures ou des recueils d'instructions de bonne pratique. Il convient que le plan de la FSA définisse ce qui doit être évalué pour le périmètre particulier de l'évaluation/du système/de l'application.
- La fréquence des FSA peut varier en fonction des différents développements de système, mais il convient qu'un minimum soit toujours fixé, avant que les dangers potentiels ne se présentent au système. Certaines sociétés aiment également conduire une évaluation avant la phase de construction/installation, pour éviter une reprise ultérieure dans le cycle de vie, coûteuse .
- Il convient que la fréquence et la rigueur de la FSA soient définies en tenant compte de certains attributs du système comme
  - la complexité;
  - l'importance de la sécurité;
  - l'expérience précédente de systèmes semblables;
  - la normalisation des caractéristiques de conception.
- Il convient qu'une justification suffisante des activités de conception, d'installation, de vérification et de validation soit disponible avant l'évaluation. La disponibilité d'une justification suffisante peut être en elle-même un critère d'évaluation. Il convient que la justification représente l'état courant/approuvé de la conception ou de l'installation du système.
- L'indépendance du ou des examinateurs doit être réelle.
- Il convient que le ou les examinateurs aient une expérience et une connaissance appropriées de la technologie et du domaine d'application du système sous évaluation.
- Il convient qu'une approche systématique et cohérente de la FSA soit maintenue tout au long du cycle de vie et pour tous les systèmes. La FSA est une activité subjective, il convient donc que des directives détaillées soient définies, probablement par l'utilisation de listes de contrôle établissant ce qui est acceptable pour une organisation, ceci afin d'éliminer dans toute la mesure du possible tout jugement subjectif.

Avant le début de la phase suivante du cycle de vie, il convient que les informations enregistrées produites à partir de la FSA soient complètes et que les conclusions soient agréées par les responsables de la gestion de la sécurité fonctionnelle concernant le SIS.

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 Le recours à une personne indépendante de l'équipe de projet a pour but d'accroître l'objectivité de l'évaluation. Le recours à une personne de haut niveau, chevronnée/confirmée, (par exemple, expérience, niveau d'éducation, position) a pour but d'assurer que les préoccupations exprimées par l'équipe de projet seront dûment prises en compte et traitées. Comme la note le suggère également, pour les équipes impliquées dans certains grands projets ou évaluations importantes, il peut être nécessaire d'avoir plusieurs personnes de haut niveau dans ces équipes, qui soient indépendantes de l'équipe de projet d'origine.

En fonction de l'organisation et de l'expertise au sein de l'entreprise, la sollicitation d'un organisme externe peut être nécessaire pour répondre à l'exigence d'un examinateur indépendant. Inversément, les entreprises disposant d'instances internes compétentes dans les domaines de l'évaluation des risques et de l'application des systèmes instrumentés de sécurité, indépendantes et distinctes (de par leur gestion et autres ressources) des instances responsables du projet, peuvent avoir la possibilité d'utiliser leurs propres ressources pour satisfaire à cette exigence d'un organisme indépendant.

5.2.6.1.3 La profondeur de l'évaluation dépend de la taille et de la complexité du projet. Il est parfois possible d'évaluer les résultats de différentes phases en même temps. Ceci est particulièrement vrai dans le cas de petites modifications à une installation industrielle en fonctionnement.

5.2.6.1.4 Dans certains pays, une évaluation de sécurité fonctionnelle entreprise à l'étape 3 est souvent nommée «Revue de sécurité de pré-démarrage» (Pre-Startup-Safety-Review ou PSSR).

5.2.6.1.5 Aucune ligne directrice n'est fournie.

5.2.6.1.6 Aucune ligne directrice n'est fournie.

5.2.6.1.7 Il convient que les membres de l'équipe d'évaluation aient accès à toutes les informations qu'ils considèrent comme nécessaires pour conduire l'évaluation. Il convient que ceci comprenne les informations issues de l'analyse de danger et de risque, de la phase de conception jusqu'à l'installation, la mise en service et la validation.

5.2.6.2 Audits et révisions

5.2.6.2.1 Ce paragraphe est prévu pour donner des directives au sujet des audits, en utilisant un exemple illustrant les activités concernées.

a) Catégories d'audits

Les audits des systèmes instrumentés de sécurité fournissent des informations intéressantes pour la direction de l'installation industrielle, pour les ingénieurs de maintenance et de conception des instruments. Ceci permet aux membres de la direction de mettre en place une gestion proactive et de se rendre compte du degré d'implication et de l'efficacité de leurs systèmes instrumentés de sécurité. De nombreux types d'audits peuvent être effectués. Il convient que le type réel, le domaine d'application et la fréquence des audits de toute activité reflète l'impact potentiel de cette dernière sur l'intégrité de sécurité.

Les types d'audits sont:

1) les audits à la fois indépendants et auto-audits;
2) les inspections;
3) les visites de sécurité (par exemple, tour de visite de l'installation industrielle et revue d'incident);
4) les enquêtes sur les systèmes instrumentés de sécurité (par l'intermédiaire de questionnaires).

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).

Une distinction doit être faite entre «la surveillance et la vérification» et les activités d'audit. La surveillance et la vérification se concentrent sur l'évaluation des performances des activités spécifiques du cycle de vie (par exemple, inspecteur vérifiant l'achèvement de l'activité de maintenance avant que le composant ne soit renvoyé pour réparation). En revanche, les activités d'audit sont plus complètes et se concentrent sur la mise en oeuvre globale des systèmes instrumentés de sécurité dans le cadre du cycle de vie de sécurité. Le fait de savoir si le programme de surveillance et de vérification a été exécuté ou non pourrait être déterminé par un audit.

Les audits et les inspections peuvent être effectués par le propre personnel de l'entreprise/du site/de l'installation industrielle/du projet, (par exemple, auto-audit) ou par des personnes indépendantes (par exemple, auditeurs de services aux entreprises, département d'assurance qualité, organismes de contrôle, clients ou tiers).

Il est possible que les membres de la direction, à divers niveaux, désirent appliquer le type adéquat d'audit pour accéder à des informations sur l'efficacité de la mise en oeuvre de leurs systèmes instrumentés de sécurité. Les informations des audits pourraient être utilisées pour identifier les procédures qui n'ont pas été correctement appliquées et conduire à une amélioration de la mise en oeuvre.

b) Stratégie d'audit

Un site/une installation industrielle/un projet mettant en œuvre des programmes d'audit peut considérer des programmes continus, indépendants ou d'auto-audit et d'inspection.

Les programmes continus sont mis à jour régulièrement pour refléter les performances des systèmes instrumentés de sécurité précédents et les résultats d'audit, les préoccupations courantes et les priorités. Ils couvrent toutes les activités et tous les aspects relatifs au site/à l'installation industrielle/au projet concernant les systèmes instrumentés de sécurité, dans une période de temps et à un degré d'approfondissement appropriés.

La raison première, et la valeur ajoutée des audits proviennent du fait qu'il est possible d'agir en temps voulu sur les informations qu'ils fournissent. Les actions visent à renforcer l'efficacité des systèmes instrumentés de sécurité, par exemple, pour aider à réduire au minimum le risque de blessure ou de mort encouru par les employés ou les personnes du public, contribuent à améliorer la culture de sécurité, à prévenir tout dégagement évitable de substance dans l'environnement.

En résumé, la stratégie d'audit peut être un panachage de différents types d'audits, conduite par la direction (le client) et a pour but de réintroduire des informations pertinentes en haut de la chaîne de direction pour initier une action en temps voulu.

c) Processus et protocoles d'audit

Le but général est d'atteindre la valeur maximale de performance de l'audit, qui ne peut être obtenue que lorsque toutes les parties (y compris auditeurs, contact désigné, directeurs de l'installation et chef de départements/services, etc.) en comprennent le besoin et peuvent influencer chaque audit. Il est possible que les processus et les protocoles d'audit suivants participent à assurer une certaine cohérence dans les démarches visant à atteindre ces objectifs. Ils portent sur les cinq principales étapes suivantes du processus d'audit:

1) Stratégie et programme d'audit

Il convient que le but de chaque audit soit clairement défini et que les groupes d'audit soient identifiés, ainsi que les rôles et les responsabilités de chacun d'eux.

Il convient qu'il y ait une stratégie pour conduire les audits.

Il convient qu'il y ait un programme d'audits.

Il convient qu'il y ait des revues régulières du processus d'audit, du programme et de la stratégie de mise en oeuvre.

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) Préparation de l'audit et pré-planification

Avant le début d'un audit, il convient qu'un cadre supérieur du site/de l'installation industrielle/du projet et/ou que le coordonnateur ad hoc de l'audit identifie un préposé aux contacts.

Il convient que les auditeurs et le préposé aux contacts, dans un premier temps, examinent, comprennent et soient d'accord sur

– le domaine d'application de l'audit;
– le calendrier d'exécution de l'audit;
– les personnes qui doivent être disponibles;
– les bases de l'audit ou la norme de l'audit;
– le fait de consentir un effort supplémentaire lors de l'étape de préparation et de faire participer le personnel de l'installation industrielle, ce qui augmentera les chances de réussite de l'audit.

Il convient de se baser sur les proportions indiquées ci-dessous pour répartir de façon appropriée le temps imparti à chaque étape:

– préparation de l'audit: 30 %;
– conduite de l'audit: 40 %;
– compte-rendu des résultats: 20 %;
– suivi de l'audit: 10 %.

Il convient que l'auditeur se prépare à l'audit en rassemblant des informations, des procédures/des instructions etc., des données, et en préparant des listes de contrôle, le cas échéant.

Il convient que l'auditeur mette en avant et explique comment un changement éventuel au domaine d'application de l'audit peut avoir lieu pendant l'audit, si des observations/des défectuosités graves sont découvertes.

3) Conduite de l'audit

L'auditeur doit conduire l'audit sur plusieurs jours consécutifs pendant la période fixée pour l'audit, en sachant pertinemment qu'il est possible que des personnes du site/de l'installation industrielle/du projet soient indisponibles.

Il convient que le préposé aux contacts soit périodiquement mis au courant des résultats identifiés pendant l'audit, évitant de ce fait des surprises à la fin de l'audit.

Il convient que l'auditeur essaie d'impliquer le personnel de l'installation industrielle dans le processus d'audit, afin de communiquer le savoir et la compréhension (du processus et des résultats) pour obtenir l'adhésion.

Le comportement de l'auditeur est crucial vis-à-vis du succès de l'audit: essayer d'être utile, constructif, courtois, objectif et d'aller en profondeur tout en étant sélectif.

Il convient au minimum, que l'auditeur essaie de respecter le domaine d'application et l'emploi du temps convenus – il sera nécessaire de négocier les variantes.

4) Compte-rendu de résultats

Il convient que l'auditeur tienne une réunion de conclusion à la fin de l'audit ou plus tard, mais avant que le compte-rendu final ne soit publié.

Il convient que des membres ad hoc de la direction aient l'opportunité de présenter leurs observations sur le projet de compte-rendu et sur les résultats, et de les discuter/commenter lors d'une réunion formelle de clôture, si cela est souhaité.

Une pratique habituelle veut qu'il soit demandé que le site/l'installation industrielle/le projet mette en place un plan d'action pour tenir compte des résultats du compte-rendu.

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) Suivi de l'audit

Les comptes-rendus d'audit requièrent habituellement une réponse sous forme de plan d'action. Il est possible que l'auditeur vérifie l'achèvement satisfaisant de l'action à la date prévue ou au prochain audit, l'échéance la plus appropriée étant choisie.

Des systèmes de suivi de site/d'installation industrielle/de projet peuvent être utilisés pour vérifier la mise en oeuvre des plans d'action.

Il convient que périodiquement une revue/un récapitulatif des résultats d'audit de chaque groupe d'audit soit considéré et que ses résultats soient largement communiqués.

Les résultats/conclusions des audits peuvent être utilisés pour réviser la fréquence des audits et constituent une entrée utile pour revoir la gestion des systèmes instrumentés de sécurité.

5.2.6.2.2 Ce paragraphe renforce le rôle que la gestion des modifications joue dans le processus d'audit.

5.2.7 Gestion de configuration du SIS

5.2.7.1 Exigences

5.2.7.1.1 Pour gérer et maintenir la traçabilité des dispositifs pendant le cycle de vie, un mécanisme pour identifier, contrôler et suivre le modèle/les versions de chaque dispositif peut être établi.

A l'étape la plus en amont possible du cycle de vie de sécurité, il convient qu'une identification unique de l'installation industrielle soit donnée à chaque dispositif. Dans certains cas, les modèles/les versions antérieurs toujours en service peuvent également faire l'objet de contrôles et de maintenance. Il convient que ce soit la première étape dans le programme de gestion de configuration qui intègre les considérations suivantes.

Le système de gestion de configuration peut inclure

a) une provision pour une procédure d'identification de tous les dispositifs pendant toutes les phases du cycle de vie;

b) l'identification unique, du modèle/de la version et de l'état à la construction de chaque dispositif comprenant le logiciel, le fournisseur, la date et si cela est applicable, les modifications du modèle/de la version spécifiées à l'origine;

c) l'identification et le suivi de toutes les actions et modifications résultant des observations des défaillances et des audits;

d) le contrôle de l'édition d'une révision entrant en service, identifiant l'état et le modèle/la version des dispositifs associés;

e) des sauvegardes qui ont été établies pour s'assurer que des changements/des modifications non autorisés ne sont pas faits au SIS, alors qu'il est en fonction;

f) l'identification des versions de tous les éléments de logiciel qui ensemble constituent une version spécifique d'un dispositif complet;

g) une provision pour la coordination de la mise à jour de plusieurs SIS dans une ou plusieurs installations industrielles;

h) l'autorisation documentée de la révision entrant en service;

i) une liste autorisée de signatures pour la révision du dispositif entrant en service;

j) les dispositifs de l'étape/de la phase qui sont présentés sous contrôle de configuration;

k) le contrôle de la documentation associée livrable;

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) l'identification de chaque modèle/version d'un dispositif;
   – spécification fonctionnelle;
   – spécification technique.
m) tous les services/départements/organismes impliqués dans la gestion et la maintenance du SIS sont identifiés et des responsabilités affectées et comprises.

6 Exigences relatives au cycle de vie de sécurité

6.1 Objectifs

Dans toute fonction de processus, la sécurité fonctionnelle obtenue dépend d'un certain nombre d'activités exécutées de manière satisfaisanteL'adoption d'une approche systématique du cycle de vie de sécurité vis-à-vis d'un système instrumenté de sécurité vise à s'assurer que toutes les activités nécessaires pour obtenir la sécurité fonctionnelle sont conduites et qu'il peut être démontré pour les autres qu'elles ont été exécutées dans un ordre approprié. La CEI 61511-1 présente un cycle de vie typique à la Figure 8 et au Tableau 2. Les exigences pour chaque phase du cycle de vie sont données par les Articles 8 à 16.

La norme admet qu'il est possible de structurer les activités spécifiées de différentes manières, à condition que toutes les exigences soient satisfaites. Cette restructuration peut être bénéfique si elle permet aux activités de sécurité d'être mieux intégrées dans les procédures habituelles du projet. Le but de l'Article 6 de la CEI 61511-1 est de s'assurer que si un cycle de vie de sécurité différent est utilisé, les entrées et la sortie de chaque phase du cycle de vie sont définies et toutes les exigences importantes sont intégrées.

6.2 Exigences

6.2.1 La considération principale consiste à définir à l'avance le cycle de vie de sécurité du SIS qui va être utilisé. L'expérience a montré que des problèmes sont susceptibles d'apparaître, sauf si cette activité est planifiée bien à l'avance et si des accords sont conclus avec toutes les personnes, services/départements et organismes qui en prennent la responsabilité. Au mieux, certains travaux seront retardés ou devront être refaits; au pire, la sécurité peut être compromise.

6.2.2 Bien que ce ne soit pas une exigence, il est généralement bénéfique, à une étape précoce, d'établir une correspondance entre le cycle de vie de sécurité du SIS proposé et le projet de cycle de vie du processus, comprenant l'identification des cases de la Figure 8 de la CEI 61511-1 qui s'appliquent au projet. Ce faisant, il convient de passer en revue avec les personnes susceptibles de pouvoir les fournir toutes les informations nécessaires pour commencer une activité du cycle de vie de sécurité.. Dans certains cas, il se peut qu'il ne soit pas possible de déterminer des informations précises sur un point particulier, jusqu'à une étape très en aval dans la phase de conception. Dans ce cas, il peut être nécessaire de faire une estimation basée sur une expérience précédente et ensuite de confirmer les données à une date ultérieure. Lorsque c'est le cas, il est important de le noter dans le cycle de vie de sécurité.

6.2.3 Une autre partie importante de la planification du cycle de vie de sécurité consiste à identifier les techniques qui seront utilisées lors de chaque phase. L'identification de ces techniques est importante, car il est souvent nécessaire d'utiliser une technique spécifique, qui nécessite des personnes ou des services/départements avec des compétences et des expériences particulières. Par exemple, les conséquences dans une application particulière peuvent dépendre de la pression maximale développée à la suite d'un cas de défaillance; la seule manière de déterminer ceci est de développer un modèle dynamique du processus. Les exigences des informations relatives à la modélisation dynamique auront alors un impact important sur le processus de conception.

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 Vérification

7.1 Objectif

Le but de la vérification est de s'assurer que les activités, pour chaque phase du cycle de vie de sécurité, comme déterminé dans le plan de vérification, ont bien été réalisées et que les sorties requises de la phase, qu'elles soient ou non sous forme de documentation, de matériel ou de logiciel, ont été générées et conviennent à l'usage qui doit en être fait.

7.1.1 Exigences

7.1.1.1 La CEI 61511-1 admet que les organismes auront leurs propres procédures de vérification et n'exigent pas d'eux qu'elles soient toujours effectuées de la même manière. Le but de ce paragraphe est plutôt de faire en sorte que toutes les activités de vérification soient planifiées à l'avance, avec toutes les procédures, les mesures et les techniques qui doivent être utilisées.

7.1.1.2 Aucune ligne directrice n'est fournie.

7.1.1.3 Il est important que les résultats de la vérification soient disponibles, de sorte qu'ils puissent démontrer qu'une vérification effective a eu lieu à toutes les phases du cycle de vie de sécurité.

8 Analyse de danger et de risque relative au processus

8.1 Objectifs

L'objectif global est ici d'établir le besoin de fonctions de sécurité (par exemple, couches de protection), ainsi que les niveaux associés de performances (réduction de risque) qui sont nécessaires pour assurer un processus sûr. Il est habituel, dans le domaine des processus, d'avoir des couches de sécurité multiples, de sorte que la défaillance d'une seule couche ne puisse pas conduire à (ou ne puisse pas permettre) l'apparition d'une conséquence néfaste. Des couches typiques de sécurité sont représentées à la Figure 9 de la CEI 61511-1.

8.2 Exigences

8.2.1 Les exigences pour l'analyse de danger et de risque ne sont spécifiées qu'en termes de résultats de la tâche. Ceci signifie qu'un organisme peut utiliser toute technique qu'il considère comme efficace, à condition qu'elle permette une description claire des fonctions de sécurité et des niveaux associés de performances.

Il convient qu'une analyse de danger et de risque identifie et tienne compte des dangers et des événements dangereux qui pourraient se produire dans toutes les circonstances raisonnablement prévisibles (y compris les conditions de défaut et un mauvais usage raisonnablement prévisible).

Sur un projet typique du domaine des processus, il est nécessaire d'effectuer une analyse de danger et de risque préliminaire, au début de la conception du processus de base. Une hypothèse à ce stade est que l'on a éliminé ou réduit les dangers autant que cela est raisonnablement réalisable, par l'application des principes de sécurité inhérents et par l'application des règles de l'art (cette activité de réduction de danger n'est pas dans le domaine d'application de la CEI 61511). Pour le SIS, cette analyse préliminaire de danger et de risque est importante parce que l'établissement, la conception et la mise en oeuvre d'un SIS sont des tâches complexes et peuvent prendre un temps considérable. Une autre raison d'entreprendre tôt ce travail est que les informations sur l'architecture du système seront nécessaires avant que les diagrammes du processus et de l'instrumentation ne soient finalisés.

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.

Habituellement, les informations seront suffisantes pour permettre l'analyse préliminaire de danger et de risque après réalisation d'un organigramme du processus aura été réalisé et mise à disposition de toutes les données du processus initial. Il convient de reconnaître que des dangers supplémentaires peuvent être mis en évidence suite aux résultats de la conception détaillée. Une analyse finale de danger et de risque peut donc être nécessaire une fois que le diagramme du processus et de l'instrumentation a été mené à bonne fin. Cette analyse finale utilise généralement une procédure formelle et entièrement documentée, telle que l'étude de risque et d'efficacité opérationnelle (HAZOP). Il convient qu'elle confirme que les couches de sécurité, telles qu'elles sont conçues, permettent d'assurer la sécurité de l'installation industrielle. Pendant cette analyse finale, il est nécessaire de considérer si des défaillances dans les systèmes de sécurité introduisent ou non de nouveaux dangers ou de nouvelles sollicitations. Si de nouveaux dangers sont révélés à ce stade, il peut être nécessaire de définir de nouvelles fonctions de sécurité. Une autre conclusion plus probable est que des événements supplémentaires soient identifiés, conduisant à des dangers qui ont déjà été identifiés à une étape préliminaire. Il sera alors nécessaire d'étudier si une révision quelconque des fonctions de sécurité et des exigences de performances, qui ont été déterminées dans l'analyse originale, est nécessaire.

L'approche utilisée pour identifier les dangers dépendra de l'application considérée. Pour certains processus simples, pour lesquels on a une longue expérience en exploitation d'une conception standard, telles que des plates-formes pétrolières simples en mer (têtes de puits), il peut être suffisant d'utiliser les listes de contrôle développées par l'industrie (par exemple, les listes de contrôle d'analyse de sécurité de l'ISO 10418 et de l'API 14C). Dans le cas où la conception serait plus complexe ou si un nouveau processus devait être étudié, une approche plus structurée pourrait être nécessaire (par exemple, CEI 60300-3-9; 1995).

NOTE D'autres informations sur le choix des techniques appropriées sont fournies par l'ISO 17776

Lorsque l'on considère les conséquences d'un cas de défaillance particulier, il convient d'étudier tous les résultats possibles et de distribuer la fréquence du cas de défaillance de manière adéquate parmi les résultats possibles. Il convient de n'ignorer aucun résultat crédible ou de le soustraire à une analyse de risque. Le fait de soumettre des conduits ou des réservoirs à des pressions supérieures à celles pour lesquelles ils ont été conçus n'aura pas toujours comme conséquence une perte catastrophique du confinement. Dans de nombreux cas, les équipements auront été soumis à une pression d'essai supérieure à la pression pour laquelle ils ont été conçus et la seule conséquence pourrait être une fuite de substances inflammables, conduisant à une possibilité d'incendie. Lors de l'évaluation des conséquences, les personnes chargées de l'intégrité mécanique de l'installation industrielle devront être consultées. Elles devront tenir compte de la pression d'essai d'origine, mais également du fait que la conception d'origine a inclus des surépaisseurs de corrosion ou non et qu'un programme de gestion de la corrosion est en place ou non. Dans le cas où les conséquences seraient fondées sur de telles hypothèses, il serait important que ceci soit clairement énoncé, de sorte que des procédures appropriées puissent être incorporées au système de gestion de la sécurité. Une autre question, lorsque l'on étudie les conséquences, sera le nombre de personnes susceptibles d'être menacées par un danger particulier. Dans bien des cas, le personnel opérationnel et de maintenance sera le seul présent dans la zone dangereuse, de manière peu fréquente et il convient d'en tenir compte en prévoyant les conséquences. Il est nécessaire de faire attention en utilisant cette approche statistique, puisqu'elle ne sera pas valide dans tous les cas, comme dans celui où le danger n'apparaît que pendant la mise en marche, alors que le personnel est toujours présent. En outre, il convient de prendre en considération l'augmentation potentielle du nombre de personnes se trouvant à proximité de l'événement dangereux pour étudier les symptômes pendant sa formation et jusqu'à l'événement lui-même.

En estimant les sources potentielles de sollicitation sur le SIS, il convient que l'évaluation englobe les situations suivantes: la mise en route, l'exploitation continue, l'arrêt, les erreurs de maintenance, les interventions manuelles (par exemple, contrôleurs sur manuel) la perte de services (par exemple, d'air, d'eau de refroidissement, d'azote, de secteur, de vapeur, de moyen de chauffage, etc.).

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.).

Lorsque l'on étudie la fréquence des sollicitations, il peut être nécessaire, dans certains cas complexes, d'entreprendre une analyse par arbre de panne. Cela est souvent nécessaire lorsque des conséquences graves ne résultent que de la défaillance simultanée de plusieurs événements (par exemple, lorsque des collecteurs de décharge ne sont pas conçus pour le pire cas, c'est-à-dire décharge de toutes les sources). Il sera nécessaire de porter un jugement à ce sujet, lorsque les erreurs de l'opérateur sont à inclure dans la liste des événements qui peuvent provoquer le danger, et d'évaluer la fréquence à utiliser pour ces événements. L'erreur de l'opérateur, en tant que sollicitation, peut souvent être exclue, si l'action est sujette à des procédures d'autorisation ou si des dispositifs de verrouillage sont fournis pour empêcher une action involontaire. Il est également nécessaire de faire attention lorsque l'on fait confiance à la réduction de la fréquence de sollicitation du fait de l'action de l'opérateur. Cette confiance sera nécessairement limitée par des considérations de facteurs humains, telles que la vitesse nécessaire à la prise de décision d'une action et la complexité des tâches impliquées. Dans le cas où un opérateur, du fait d'une alarme, entreprendrait une action, la réduction de risque revendiquée étant supérieure à un facteur 10, le système global devra alors être conçu en accord avec la CEI 61511-1. Le système chargé de la fonction de sécurité comporterait alors le capteur détectant la condition dangereuse, la présentation de l'alarme, la réponse de l'opérateur humain et les équipements utilisés par ce dernier pour mettre fin à tout danger. Il convient de noter qu'une réduction de risque jusqu'à un facteur 10 pourrait être déclarée, sans la nécessité de se conformer à la CEI 61511. Dans le cas où de telles déclarations seraient faites, les questions de facteur humain devraient être soigneusement étudiées. Il convient que toutes les revendications relatives à la réduction de risque, suite à une alarme, s'appuient sur une description documentée de la réponse nécessaire à l'alarme et qu'un temps suffisant soit laissé à l'opérateur pour engager l'action corrective et l'assurance que l'opérateur sera formé pour prendre des mesures préventives.

Un système d'alarme peut être utilisé comme méthode de réduction de risque en réduisant le taux de sollicitation sur le SIS à condition que

– le capteur employé pour le système d'alarme ne soit pas utilisé dans un but de contrôle, où la perte de contrôle conduirait à une sollicitation sur la SIF;
– le capteur utilisé pour le système d'alarme ne soit pas utilisé en tant qu'élément du SIS;
– qu'il soit tenu compte des limitations relatives à la réduction de risque qui peuvent être revendiquées pour le BPCS et les questions de cause commune.

Des exemples de techniques pouvant être utilisées pour établir le SIL des systèmes instrumentés de sécurité sont donnés par la CEI 61511-3, qui contient également des directives sur les considérations à prendre en compte lors du choix de la méthode à utiliser pour une application spécifique.

En établissant si la réduction de risque est requise ou non, il est nécessaire d'avoir une certaine cible de sécurité pour le processus et une cible environnementale. Celles-ci peuvent être spécifiques au site particulier ou à l'entreprise d'exploitation et seront comparées au niveau du risque sans fonction supplémentaire de sécurité. Après avoir établi le besoin de réduction de risque, il faudra considérer quelles sont les fonctions qu'il est nécessaire d'exécuter pour que le processus revienne à un état de sécurité. En théorie, les fonctions peuvent être décrites d'une façon générale, sans référence à une technologie particulière. Dans le cas d'une protection de surpression par exemple, la fonction peut être décrite comme un moyen de prévention contre l'élévation de pression au-dessus d'une valeur spécifiée. Soit une soupape de sécurité, soit un système instrumenté de sécurité pourrait alors remplir cette fonction. Si la fonction est décrite comme ci-dessus, le choix du type de technologie à utiliser sera décidé lors de l'étape suivante du cycle de vie (allocation des fonctions de sécurité aux couches de protection). En pratique, les exigences fonctionnelles seraient différentes selon le type de système choisi; cette étape et la suivante, peuvent dans certains cas être combinées.

En résumé, il convient que l'analyse de danger et de risque considère ce qui suit:

– chaque événement dangereux déterminé et les séquences d'événements qui y contribuent;

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 SIF;
- 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;

– les conséquences et la vraisemblance des séquences d'événements avec lesquelles chaque événement dangereux est associé; celles-ci peuvent être exprimées quantitativement ou qualitativement;

– la réduction nécessaire de risque pour chaque événement dangereux;

– les mesures prises pour réduire ou éliminer les dangers et les risques;

– les hypothèses faites pendant l'analyse des risques, y compris les taux estimés de sollicitation et les taux de défaillance des équipements; il convient de détailler toute prise en compte des contraintes opérationnelles ou des interventions humaines;

– les références aux informations importantes qui se rapportent aux systèmes sécuritaires, à chaque phase du cycle de vie du SIS (par exemple, les activités de vérification et de validation).

Il convient que les informations et les résultats qui constituent l'analyse de danger et de risque soient documentés.

Il peut être nécessaire, que l'analyse de danger et de risque soit répétée à différentes étapes du cycle de vie global de sécurité du SIS, car des décisions sont prises, et les informations disponibles deviennent plus précises.

8.2.2 Dans la production industrielle par processus, une cause importante de sollicitations, qui devra être considérée dans de nombreuses applications, est la défaillance du BPCS. Il convient de noter que la défaillance du BPCS peut être provoquée par le capteur, la vanne ou le système de commande.

Parfois, les systèmes de commande utilisés dans la production industrielle par processus ont des processeurs redondants, mais les capteurs et les vannes ne le sont généralement pas. Lorsque l'on affecte un taux de défaillance au BPCS, une limitation importante doit être prise en compte. La CEI 61511-1 limite le taux des défaillances dangereuses, par rapport à un risque particulier, à 10^{-5} par heure, sauf si le système est mis en application selon les exigences de cette norme. La raison de la limite est que si un taux de défaillances dangereuses inférieur est déclaré, il se situe dans la plage des taux de défaillance du Tableau 4. La limite garantit que des niveaux de confiance élevés ne sont pas affectés à des systèmes qui ne satisfont pas aux exigences de la CEI 61511-1.

8.2.3 Aucune ligne directrice n'est fournie.

9 Allocation des fonctions de sécurité aux couches de protection

9.1 Objectif

Afin de déterminer les besoins pour un SIS et son SIL associé, il est important de considérer si d'autres couches de protection existent (ou doivent exister) et quelle protection elles assurent. Après avoir considéré les autres couches de protection, il convient alors de déterminer la nécessité d'une couche de protection pour le SIS. Si une couche de protection pour le SIS est nécessaire, il convient alors de déterminer le SIL pour la (les) fonction(s) instrumentée(s) de sécurité de ce SIS.

9.2 Exigences relatives au processus d'allocation

9.2.1 L'exigence consiste à convenir des couches de sécurité à utiliser et à assigner des cibles de performances pour les fonctions instrumentées de sécurité. En pratique et dans de nombreux cas, les fonctions de sécurité ne sont assignées qu'aux systèmes instrumentés de sécurité présentant des problèmes lorsqu'ils utilisent des conceptions à sécurité intrinsèque ou des systèmes avec d'autres technologies.

- 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.

Des exemples de ces problèmes comprennent les limitations concernant la capacité de formation de torchères ou la protection contre des réactions exothermiques. Toute décision d'utiliser des systèmes à base d'instruments plutôt que des approches plus traditionnelles telles que des soupapes de sécurité, devra être justifiée par de bonnes raisons qui s'opposeront aux organismes de réglementation.

Comme cela est mentionné ci-dessus, l'évaluation et l'allocation de danger et de risque peuvent être des activités simultanées ou bien l'allocation peut, dans certaines circonstances, avoir lieu avant l'évaluation de danger et de risque. Les décisions concernant l'allocation des fonctions de sécurité aux couches de sécurité sont souvent prises sur la base de ce qui s'est avéré réalisable par l'organisme de l'utilisateur. Il convient que la bonne pratique industrielle en la matière soit également prise en considération. Les décisions concernant les systèmes instrumentés de sécurité seront alors prises, en prenant en compte les performances des autres couches de sécurité. Par exemple, dans le cas où des soupapes de sécurité auraient été installées et auraient été conçues et montées selon les bonnes pratiques industrielles, il pourrait alors être décidé qu'elles conviennent à elles seules, pour obtenir la réduction de risque ad hoc. Les systèmes instrumentés de sécurité limiteraient alors uniquement la pression, si le dimensionnement ou les performances de la (des) soupape(s) de sécurité était insuffisant pour l'application ou si le dégagement dans l'atmosphère doit être proscrit.

9.2.2 Aucune ligne directrice n'est fournie.

9.2.3 Lorsqu'une fonction de sécurité est affectée à une fonction instrumentée de sécurité, il est nécessaire de considérer si l'application est un mode de sollicitation ou un mode continu. La majorité des applications dans le domaine des processus opèrent en mode de sollicitation, avec des sollicitations peu fréquentes. Dans ces cas, le Tableau 3 de la CEI 61511-1 donne les valeurs appropriées à utiliser. Il y a certaines applications où les sollicitations sont fréquentes (par exemple, supérieures à une par an), et il est plus approprié de considérer l'application en tant que mode continu, parce que la probabilité de défaillances dangereuses sera principalement déterminée par le taux de défaillance du SIS. Dans ces cas, le Tableau 4 de la CEI 61511-1 donne les valeurs appropriées à appliquer. Les applications en mode continu, où la défaillance aurait comme conséquence un danger immédiat, sont rares. Une commande de brûleur ou de vitesse de turbine peuvent être des applications en mode continu, si les systèmes de protection sont insuffisants pour tous les modes de défaillance du système de commande.

Le Tableau 3 définit le SIL en termes de PFD_{avg} (Probabilité de défaillance moyenne cible lors d'une sollicitation). La PFD_{avg} cible sera déterminée par la réduction de risque requise. La réduction de risque requise peut être déterminée en comparant le risque du processus sans SIS avec le risque tolérable. Ceci peut être déterminé sur une base quantitative ou qualitative en utilisant les techniques de la CEI 61511-3.

Le Tableau 4 définit le SIL, en termes de fréquence cible de défaillances dangereuses, pour exécuter la SIF. Ceci sera déterminé par le taux de défaillance tolérable du SIS, en tenant compte des conséquences de la défaillance dans une application particulière. Lorsque le Tableau 4 est utilisé pour déterminer le SIL requis, la cible est basée sur la fréquence de la défaillance dangereuse pour le système instrumenté de sécurité. Lors de l'utilisation du Tableau 4, il est incorrect de convertir la fréquence des défaillances dangereuses en probabilité de défaillances dangereuses sur sollicitation en utilisant l'intervalle entre tests périodiques ou le taux de sollicitation. Alors que les unités peuvent sembler être correctes, il en résulte une conversion inadéquate du Tableau 4 et cela peut avoir comme conséquence une sous-spécification des exigences du SIL de la fonction de sécurité.

Les cibles de probabilité moyenne des défaillances sur sollicitation, ou de fréquence des défaillances dangereuses par heure, s'appliquent à la fonction instrumentée de sécurité et ne s'appliquent pas aux différents composants ou sous-ensembles. Un composant ou un sous-ensemble (par exemple, un capteur, une unité logique, un élément terminal) ne peut pas avoir un SIL qui lui est affecté en dehors de son utilisation dans une SIF spécifique. Cependant, il peut avoir une déclaration des possibilités maximales du SIL, indépendante.

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 61511-1defines 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 61511-1defines 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.

Il convient que les résultats du processus d'analyse et d'allocation de danger et de risque consistent en une description claire des fonctions à exécuter par les systèmes de sécurité, y compris les systèmes instrumentés de sécurité potentiels, assortie des exigences du niveau d'intégrité de sécurité (avec le mode d'exploitation, en continu ou en sollicitation) pour toute fonction instrumentée de sécurité. Ceci constitue la base de la spécification des exigences concernant la sécurité du SIS. Il convient que la description des fonctions soit claire, quant aux besoins qui doivent être satisfaits pour s'assurer que la sécurité est maintenue.

A cette étape de la mise en oeuvre, il est inutile de spécifier les détails architecturaux concernant les capteurs et les vannes. Les décisions relatives aux architectures sont complexes et définir si un système particulier nécessite ou non des capteurs 2oo3 et des vannes 1oo2 dépendra de nombreux facteurs.

9.2.4 Les implications des Tableaux 3 et 4 de la CEI 61511-1 nécessitent d'être totalement comprises. En particulier, la PFD_{avg}, qui peut être déclarée pour une fonction instrumentée de sécurité simple, est limité à 10^{-5}, correspondant à une réduction de risque de 10^5 (SIL 4). L'analyse de fiabilité peut indiquer qu'il est possible d'atteindre une PFD_{avg} de moins de 10^{-5}, dû aux défaillances aléatoires de matériel, mais la CEI 61511-1 suppose que les défaillances systématiques et les défaillances de mode commun limiteront les performances réelles qui peuvent être obtenues. Dans le cas où l'analyse de risque montrerait qu'une aussi forte réduction de risque est nécessaire, il conviendrait de noter – cela est vivement recommandé – la difficulté de réaliser une fonction instrumentée de sécurité de SIL 4, dans le domaine des processus. Il conviendrait également d'attirer l'attention sur le fait d'utiliser plusieurs SIS indépendants, d'intégrité inférieure.

Concernant la Note 4:

Plusieurs SIS peuvent être utilisés afin d'atteindre des niveaux de réduction de risque plus élevés (par exemple, supérieurs à 10^3). Lors de l'utilisation de plusieurs SIS pour atteindre une réduction de risque plus élevée, il est important que chacun des SIS puisse indépendamment exécuter la fonction de sécurité et qu'il y ait une indépendance suffisante entre les SIS. Par exemple, il ne serait pas recommandé de combiner une boucle de capture de pression de SIL 2 avec une boucle de capture de niveau de SIL 1, pour exécuter une fonction de sécurité de surpression ayant une prescription de réduction de risque de 10^3, parce qu'avant que le capteur de niveau n'ait détecté un niveau élevé, le réservoir pourrait déjà avoir dépassé ses contraintes de pression.

En outre, lorsque plusieurs SIS sont utilisés, il convient de tenir compte des défaillances de cause commune. En plus, il convient que toutes les autres exigences définies dans la CEI 61511-1 soient satisfaites, y compris les exigences minimales de tolérance aux anomalies définies par le Tableau 5.

L'exemple suivant illustre la façon dont la combinaison de plusieurs SIS pourrait être utilisée pour atteindre des niveaux de réduction de risque plus élevés.

Soient ensemble transmetteur 2oo3, une unité logique 2oo3 et un ensemble élément terminal 1oo2, ce qui donne un SIS avec une PFD_{avg} de $3{,}05 \times 10^{-4}$. Ce SIS atteint une réduction de risque d'approximativement $3{,}3 \times 10^3$.

Il serait incorrect de supposer qu'en utilisant conjointement deux de ces systèmes, il en résulterait une réduction de risque de 10×10^6 ($3{,}3 \times 10^3 \times 3{,}3 \times 10^3$). Les facteurs de cause commune, tels que l'utilisation de technologies similaires, la conception des deux systèmes à partir de la même spécification fonctionnelle, les facteurs humains (par exemple, programmation, installation, maintenance), les facteurs externes (par exemple, la corrosion, les branchements, le gel sur les lignes aériennes, la foudre) limiteront l'amélioration du système. Il serait également nécessaire de tenir compte de tous les composants partagés entre les deux systèmes.

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.

Une solution plus facilement réalisable peut consister à utiliser un deuxième système non redondant, en utilisant des composants aussi divers que possible (afin de réduire au minimum les problèmes potentiels de cause commune).

Par exemple, considérons un SIS comportant un unique commutateur, une logique à relais et un élément terminal unique, ce qui donne un système avec une PFD_{avg} de $7,7 \times 10^{-3}$. Ce SIS atteint une réduction de risque d'approximativement $1,3 \times 10^{2}$.

En combinant un SIS basé sur un logiciel avec le SIS à relais non redondant, on obtient une réduction de risque théorique globale de $4,3 \times 10^{5}$ ($3,3 \times 10^{3} \times 1,3 \times 10^{2}$). Alors que combiner les performances, comme cela est présenté ci-dessus, semble être théoriquement possible (puisque l'un des SIS pourrait arrêter l'installation de processus), il doit être, une fois encore, tenu compte des facteurs de cause commune, et la réduction de risque obtenue sera légèrement inférieure, du fait de ces facteurs.

Aucune ligne directrice n'est fournie.

9.3 Exigences supplémentaires pour le niveau 4 d'intégrité de sécurité

9.3.1 Aucune ligne directrice n'est fournie.

9.3.2 Aucune ligne directrice n'est fournie.

9.4 Exigences relatives au système de commande de processus de base en tant que couche de protection

9.4.1 Le système de commande processus de base peut être identifié en tant que couche de protection suivant certaines conditions. Si les fonctions sont mises en oeuvre dans le BPCS dans le but de réduire le risque du processus, une réduction de risque peut être allouée au BPCS pour les risques identifiés qu'il est censé réduire.

9.4.2 Une réduction de risque inférieure à 10 peut être demandée aux systèmes instrumentés, sans nécessité de se conformer à la CEI 61511-1. Ceci permet au BPCS d'être utilisé pour une certaine réduction de risque, sans qu'il soit nécessaire de mettre en oeuvre de tels systèmes avec les exigences de la CEI 61511-1. Il convient de justifier toute revendication faite par la considération de l'intégrité du BPCS (déterminé par analyse de fiabilité ou données de performances) et des procédures utilisées pour la configuration, les modifications, l'exploitation et la maintenance. En allouant la réduction de risque aux fonctions du BPCS, il est important de s'assurer qu'une sécurité d'accès et une gestion des modifications sont fournies. La réduction de risque, qui peut être revendiquée pour une fonction du BPCS, est également déterminée par le degré d'indépendance entre la fonction du BPCS et la cause primaire. La Figure 2 illustre l'indépendance de la fonction du BPCS et de la cause primaire.

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.

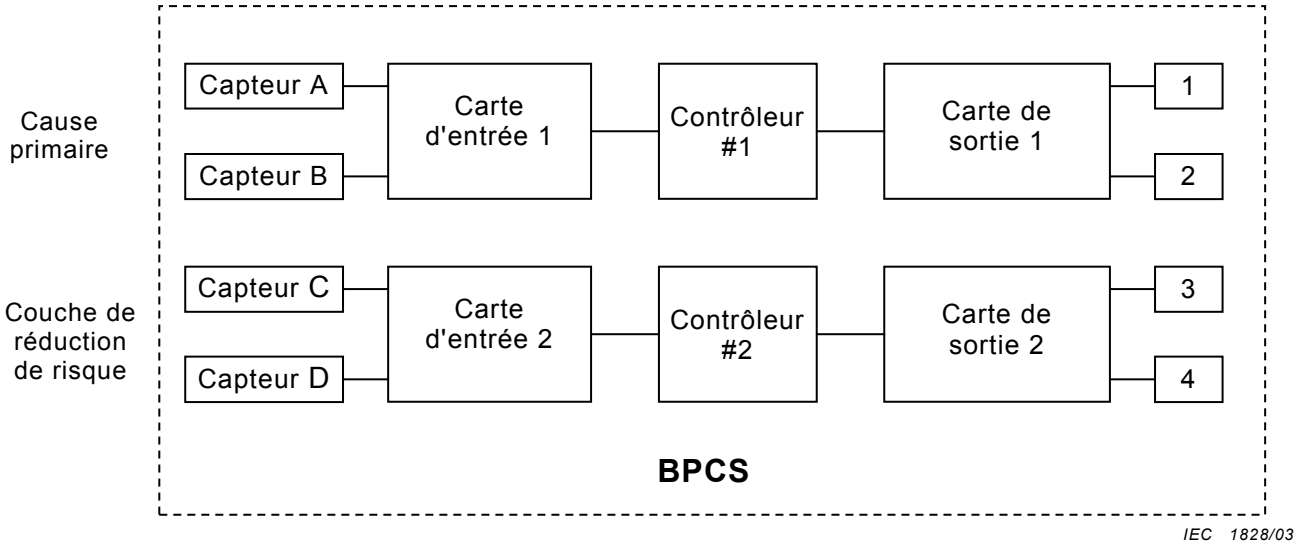


Figure 2 – Illustration de l'indépendance de la fonction du BPCS et de la cause primaire

Par exemple, considérons le cas où une boucle de commande de débit est la cause primaire. Cette cause primaire inclut un transmetteur de débit, un contrôleur, et une vanne de commande. Afin d'allouer la réduction de risque à une boucle de commande de pression du BPCS, il convient que le transmetteur de pression soit câblé à un contrôleur indépendant, modulant un élément terminal indépendant (par exemple, une vanne de mise à l'air libre d'une torchère).

9.4.3 Aucune ligne directrice n'est fournie.

9.5 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes

9.5.1 Une question importante à considérer à une étape précoce est de savoir s'il existe ou non des défaillances de cause commune entre les parties redondantes de chaque couche (par exemple, entre 2 soupapes de sécurité de surpression sur le même réservoir), entre couches de sécurité ou entre les couches de sécurité et le BPCS. Un exemple de ceci pourrait être le suivant: lorsqu'une défaillance de mesure d'un système de commande de processus de base peut provoquer une sollicitation sur le système instrumenté de sécurité et qu'un dispositif, avec les mêmes caractéristiques, est utilisé dans le système instrumenté de sécurité. Dans de tels cas, il sera nécessaire d'établir s'il y a des modes de défaillance crédibles qui pourraient provoquer la défaillance des deux dispositifs en même temps. Dans le cas où une cause de défaillance commune serait identifiée, les actions suivantes pourraient alors être entreprises.

a) La cause commune peut être réduite en modifiant la conception du système instrumenté de sécurité ou du système de commande de processus de base. La diversité de la conception et la séparation physique sont deux méthodes efficaces pour réduire la probabilité des défaillances de cause commune. C'est habituellement l'approche préférée.

b) Il convient de prendre en considération la vraisemblance de l'événement de cause commune lorsque l'on détermine si la réduction de risque globale est adéquate ou non. Ceci peut faire appel à une analyse par arbre de panne, qui inclut les causes de sollicitation, ainsi que les défaillances du système de protection. Les défaillances de cause commune peuvent être représentées sur ces arbres de panne et leur effet sur le risque global peut être quantifié par l'intermédiaire de méthodes de modélisation appropriées.

Il convient de noter que tous les capteurs ou actionneurs, qui sont partagés par le BPCS et le SIS, sont tout à fait susceptibles d'introduire des défaillances de cause commune et il convient qu'un tel partage de dispositifs soit approché comme cela est mentionné dans cet article.

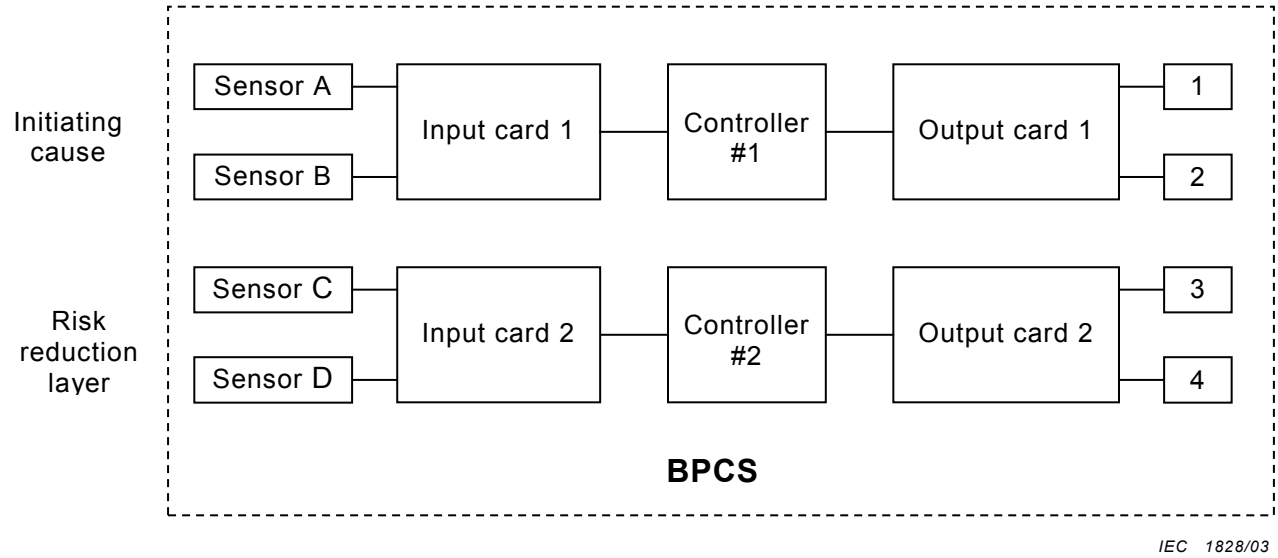


Figure 2 – BPCS function and initiating cause independence illustration

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 Les considérations énumérées ci-dessous s'appliquent lorsqu'une évaluation est effectuée sur la vraisemblance des défaillances de cause commune, de mode commun et dépendantes. L'ampleur, la forme et la profondeur de l'évaluation dépendront du niveau d'intégrité de sécurité de la fonction envisagée. L'effet des défaillances de cause commune, de mode commun et dépendantes peut être dominant pour des niveaux d'intégrité de sécurité de 3 ou supérieurs. Il convient que les points suivants soient étudiés:

– l'indépendance entre les couches de protection – il convient d'effectuer une analyse des modes de défaillance et de leurs effets pour établir si un événement unique peut provoquer la défaillance de plus d'une couche de protection ou la défaillance du BPCS et d'une couche de protection. La profondeur et la rigueur de l'analyse dépendront du risque.
– la diversité entre les couches de protection – il convient que le but soit la diversité entre les couches de protection et le BPCS, mais ceci n'est pas toujours réalisable. Un exemple pourrait être une protection de surpression, où une défaillance de la boucle de commande de pression du BPCS entraînerait une sollicitation. Le BPCS et le SIS nécessiteront tous les deux une mesure de pression et il y aura une limite pour les équipements appropriés disponibles. Une certaine diversité peut être obtenue en utilisant des équipements de différents constructeurs, mais si les capteurs du SIS et du BPCS sont connectés au processus en utilisant le même type de branchement, alors la diversité peut être de valeur limitée.
– la séparation physique entre les différentes couches de protection – la séparation physique réduira l'impact des défaillances de cause commune dues aux causes physiques. Il convient que les localisations des connexions de mesure pour le BPCS et le SIS soient données pour une séparation physique maximale, suivant les besoins fonctionnels, tels que précision et temps de réponse.

10 Spécification des exigences concernant la sécurité d'un SIS

10.1 Objectif

Le développement de la spécification des exigences concernant la sécurité du SIS est l'une des activités les plus importantes de tout le cycle de vie de sécurité. C'est par l'intermédiaire de cette spécification que l'utilisateur peut définir la manière dont il souhaite que les fonctions instrumentées de sécurité (SIF) soient conçues et intégrées dans un SIS.

Cette spécification constitue également le document de référence principal qui est utilisé pour la validation finale, montrant que toutes les exigences de la SIF ont été satisfaites.

10.2 Exigences générales

10.2.1 La spécification des exigences concernant la sécurité du SIS peut être un document unique ou un ensemble de plusieurs documents comprenant des procédures, des schémas ou des normes/règlements internes à l'entreprise. Ces exigences peuvent être développées par l'équipe d'analyse de danger et de risque et/ou par l'équipe de projet elle-même.

10.3 Exigences concernant la sécurité du SIS

10.3.1 Comme cela est décrit dans la CEI 61511-1, un certain nombre d'exigences de conception doivent être définies au début d'un projet pour s'assurer que les fonctions instrumentées de sécurité apportent la protection désirée.

Les spécifications des exigences concernant la sécurité relatives à des sous-systèmes individuels peuvent également être dérivées de cette spécification globale.

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.

10 SIS safety requirements specification

10.1 Objective

The development of the SIS safety requirements specification is one of the more important activities of the whole safety lifecycle. It is through this specification that the user is able to define how he wants the Safety Instrumented Functions (SIF) to be designed and integrated into a SIS.

Final validation of the SIS is carried out using this specification.

10.2 General requirements

10.2.1 The SIS safety requirements specification may be a single document or a collection of several documents including procedures, drawings or corporate standard practices. These requirements may be developed by the Hazard and Risk Assessment team and/or the project team itself.

10.3 SIS safety requirements

10.3.1 As described in IEC 61511-1, there are a number of design requirements that need to be defined early in a project to ensure the Safety Instrumented Functions provide the desired protection.

Safety requirements specifications for individual subsystems may also be derived from this overall specification.

Certaines considérations se rapportant aux spécifications des exigences concernant la sécurité sont les suivantes:

a) Le premier point qui devra être défini est la fonction instrumentée de sécurité avec son niveau d'intégrité de sécurité (SIL). Un exemple d'une fonction instrumentée de sécurité est de «protéger le réacteur contre une surpression en fermant les vannes d'admission sur la haute pression». Généralement la description de la fonction comportera les éléments suivants:

   - les mesures qui doivent être faites pour détecter le début des conditions dangereuses. Un exemple simple pourrait être le fait qu'une élévation de pression au-dessus d'une valeur spécifiée doive être détectée. La valeur du paramètre auquel il convient qu'une action soit entreprise devra être en dehors de la plage de fonctionnement normal et inférieure à la valeur qui aura comme conséquence la condition dangereuse. Une allocation devra être faite pour la réponse du système et pour la précision de la mesure. En fixant la limite, une discussion sera nécessaire avec les personnes responsables de la conception et de la mise en oeuvre du système instrumenté de sécurité;
   - les actions qui doivent être entreprises et qui préviendront la condition dangereuse. Un exemple simple pourrait être de diminuer le débit de vapeur vers un rebouilleur en un temps spécifié. Il convient de noter qu'il n'est habituellement pas suffisant d'énoncer que le débit de vapeur vers le rebouilleur doit être interrompu. Le concepteur devra savoir ce qui est nécessaire pour obtenir une exploitation satisfaisante. Dans des services de chauffage, par exemple, il peut être suffisant de réduire le débit à moins de 10 % dans un délai d'une minute. Dans d'autres exemples, il peut être nécessaire d'avoir une fermeture étanche, en quelques secondes;
   - les actions non nécessaires pour prévenir la condition dangereuse, qui peuvent être bénéfiques pour des raisons opérationnelles. Ces actions peuvent inclure la présentation des alarmes, l'arrêt d'unités en amont ou en aval pour réduire des sollicitations vis-à-vis d'autres systèmes de protection ou des actions qui permettront un démarrage rapide une fois que la cause du danger aura été éliminée. Il est important de séparer ces actions des actions nécessaires pour prévenir la condition dangereuse, de manière à minimiser les coûts et à restreindre la frontière du système instrumenté de sécurité à ce qui est nécessaire. Plus la frontière est grande, plus il sera difficile de prouver que la probabilité globale de défaillance sur sollicitation satisfait aux exigences associées au niveau d'intégrité spécifié.
   - tous les états ou séquences du processus identifiés relatifs à l'exploitation du SIS, qu'il convient d'empêcher parce qu'ils auront comme conséquence des situations dangereuses.

b) il convient que cette spécification définisse l'état de sécurité du processus pour chaque fonction identifiée en termes de débits qui devraient être initiés ou arrêtés, de vannes du processus qui devraient être ouvertes ou fermées et d'état de fonctionnement de tous les équipements tournants (pompes, compresseurs, agitateurs). Si le fait d'amener le processus à un état de sécurité implique un séquencement, il convient que ce dernier soit également identifié;

   NOTE En définissant les éléments terminaux, il convient de porter attention aux avantages de la diversité, par exemple, en coupant le flux de produit et en arrêtant le débit de vapeur pour réduire la haute pression.

c) il convient de définir, au début, la prescription pour un intervalle de tests périodiques désiré, ainsi la conception du SIS peut le prendre en compte. Par exemple, si les tests périodiques sont à exécuter pendant des arrêts planifiés (par exemple, tous les 3 ans), la conception pourrait requérir plus de redondance que si l'intervalle des tests périodiques est annuel;

d) il convient de définir les exigences pour pouvoir amener manuellement le processus à un état de sécurité. Par exemple, s'il y a une prescription pour que l'opérateur puisse manuellement arrêter un équipement à partir, soit de la salle de commande, soit d'un endroit sur le terrain, ceci nécessite alors d'être spécifié. Toute prescription relative à l'indépendance des commutateurs manuels d'arrêt à partir de l'unité logique du SIS nécessite également d'être définie;

Some considerations with respect to the safety requirements specifications are as follows:

a) The first items that will need to be defined is the safety instrumented function along with its Safety Integrity Level (SIL). An example of a Safety Instrumented Function is “protect the reactor from overpressure by shutting down the inlet valves on high pressure”. Typically the function description will comprise the following elements.

   - Which measurements need to be taken to detect the onset of the hazardous conditions. A simple example could be that a pressure rise above a specified value needs to be detected. The value of the parameter at which action should be taken will need to be outside the normal operating range and less than the value that will result in the hazardous condition. An allowance will need to be made for the response of the system and the accuracy of measurement. In setting the limit, there will therefore need to be a discussion with those responsible for the safety instrumentation system design and implementation.
   - The actions that need to be taken that will prevent the hazardous condition. A simple example could be to reduce the flow of steam to a reboiler within a specified time. It should be noted that it is not usually sufficient to state that steam flow to the reboiler should be shut-off. The designer will need to know what is necessary for successful operation. In heating duties it may for example be sufficient to reduce flow to less than 10 % of flow within one minute. In other examples it may be necessary to have tight shut-off within a few seconds.
   - The actions not needed to prevent the hazardous condition that may be of benefit for operational reasons. Such actions may include presentation of alarms, shut down of upstream or downstream units to reduce demands on other protection systems or actions that will enable fast start up once the cause of the hazard has been eliminated. It is important to separate these actions from the actions necessary to prevent the hazardous condition so as to minimize costs and restrict the boundary of the safety instrumented system to what is necessary. The wider the boundary is set, the more difficult it will be to show that the overall probability of failure on demand meets the requirements associated with the specified integrity level.
   - Any identified process states or sequences of the SIS operation which should be prevented because they will result in hazardous situations.

b) This specification should define the safe state of the process for each identified function in terms of which flows should be started or stopped, which process valves should be opened or closed and the state of operation of any rotating equipment (pumps, compressors, agitators). If bringing the process to a safe state involves sequencing, the sequencing should also be identified.

   NOTE In defining the final elements, consideration should be given to the benefits of diversity, for example, shutting off the product stream and shutting off the steam flow to reduce high pressure.

c) The requirement for a desired proof test interval should be defined at the beginning so the design of the SIS can take it into consideration. For example, if proof testing is to be performed during planned shutdowns (for example, every 3 years), the design might require more redundancy than if the proof test interval is to be annual.

d) Requirements for being able to manually bring the process to a safe state should be defined. For example, if there is a requirement for the operator to be able to manually shutdown a piece of equipment from either the control room or from a field location, then this needs to be specified. Any requirement for independence of manual shutdown switches from the SIS logic solver also needs to be defined.

e) toutes les exigences pour remettre en marche le processus après un arrêt nécessitent d'être spécifiées. Par exemple, certains utilisateurs ont des commutateurs électroniques de réinitialisation sur le panneau de commande principal ou sur le terrain et d'autres aiment utiliser des solénoïdes avec des manettes de verrouillage. S'il y a une prescription spécifique, comme cette action de réinitialisation, il convient qu'elle fasse partie de la spécification des exigences concernant la sécurité;

f) s'il y a une fréquence cible pour les déclenchements intempestifs, il convient qu'elle soit aussi définie par la spécification des exigences concernant la sécurité. Ceci sera un facteur à prendre en compte dans la conception du SIS;

g) les interfaces entre le SIS et l'opérateur nécessitent d'être totalement décrites, y compris les alarmes (alarmes préliminaires à l'arrêt, alarmes d'arrêt, alarmes de dérivation, alarmes des dispositifs de diagnostic), les graphiques, l'enregistrement des séquences d'événements;

h) il peut être nécessaire d'avoir des dérivations pour permettre au SIS d'être essayé ou maintenu, pendant que le processus s'exécute. En cas d'exigences spécifiques pour des dérivations de dispositifs, comme un interrupteur à clé ou des mots de passe, celles-ci doivent également être précisés en tant qu'éléments de la spécification des exigences concernant la sécurité;

i) il convient de définir les modes de défaillance et la réponse du SIS sur la détection des anomalies. Par exemple, un transmetteur peut être conçu pour passer en défaillance en allant vers une condition de déclenchement ou en partant d'une condition de déclenchement. S'il est conçu pour passer en défaillance en partant de la condition de déclenchement, il est alors important que l'opérateur obtienne une alarme lors de la défaillance du transmetteur et qu'il soit formé pour entreprendre l'action corrective nécessaire pour que le transmetteur soit réparé aussi rapidement que possible. Voir également le Paragraphe 11.3 de la CEI 61511-1, qui concerne les exigences relatives à la détection d'une anomalie.

10.3.2 Aucune ligne directrice n'est fournie.

11 Conception et ingénierie du SIS

11.1 Objectif

L'objectif de cet article est de donner des directives concernant la conception du SIS. Chaque SIF a son propre SIL. Un composant d'un SIS, par exemple, une unité logique, peut être utilisé par plusieurs SIF avec différent SIL.

11.2 Exigences générales

11.2.1 Aucune ligne directrice n'est fournie.

11.2.2 Aucune ligne directrice n'est fournie.

11.2.3 Aucune ligne directrice n'est fournie.

11.2.4 L'Article 11 de la CEI 61511–1, donne un certain nombre d'exigences de conception pour un SIS. Un sujet de préoccupation est l'indépendance entre le SIS et le BPCS.

Un système instrumenté de sécurité est généralement distinct du BPCS pour les raisons suivantes:

a) pour réduire les effets du BPCS sur le SIS, particulièrement lorsqu'ils partagent des équipements communs. Par exemple si les BPCS et SIS partagent une vanne commune pour l'arrêt et la commande, en cas de défaillance dangereuse de cette dernière, elle ne serait pas disponible pour exécuter une fonction d'arrêt du SIS;

e) All requirements for restarting the process after a shutdown need to be specified. For example, some users have electronic reset switches on the main control panel or in the field and others like to use solenoids with latching handles. If there is a specific requirement like this reset action, it should be part of the safety requirements specification.

f) If there is a target frequency for nuisance trips, this also should be specified as part of the safety requirements specification. This will be a factor in the design of the SIS.

g) The interfaces between the SIS and the operator need to be fully described, including alarms (pre-shutdown alarms, shutdown alarms, bypass alarms, diagnostic alarms), graphics, sequence of events recording.

h) There may be a need for bypasses to allow the SIS to be tested or maintained while the process is running. If there are specific requirements for bypassing such devices as key lock or passwords, these also need to be specified as part of the safety requirements specification.

i) The failure modes and response of the SIS on the detection of faults should be defined. For example, a transmitter can be designed to fail toward a trip condition or away from a trip condition. If it is designed to fail away from the trip condition, then it is important that the operator gets an alarm on the transmitter failure and is trained to take the necessary corrective action to get the transmitter repaired as quickly as possible. See also IEC 61511-1, 11.3 relating to requirements on detection of a fault.

10.3.2 No further guidance provided.

11 SIS design and engineering

11.1 Objective

The objective of this subclause is to provide guidance in the design of the SIS. Each SIF has its own SIL. A component of a SIS, for example, a logic solver, may be used by several SIFs with different SILs.

11.2 General requirements

11.2.1 No further guidance provided.

11.2.2 No further guidance provided.

11.2.3 No further guidance provided.

11.2.4 IEC 61511–1, Clause 11, has a number of design requirements for a SIS. One item of concern is independence between the SIS and the BPCS.

A SIS is normally separated from the BPCS for the following reasons:

a) To reduce the effects of the BPCS on the SIS, especially when they share common equipment. For example if the BPCS and SIS share a common valve for shutdown and control, then in the event of a dangerous failure of that valve, it would not be available to perform a SIS shutdown function.

b) pour permettre de faire plus facilement des modifications, assurer la maintenance, les essais et mettre à jour la documentation du BPCS;

NOTE 1 Le SIS a généralement des exigences plus sévères que le BPCS et le but n'est pas de soumettre le BPCS aux mêmes exigences sévères que celles qui sont exigées pour le SIS. Cependant, il convient de noter que les modifications non contrôlées du BPCS peuvent être la cause d'une augmentation des sollicitations sur le SIS.

c) pour faciliter la validation et l'évaluation fonctionnelle de sécurité du SIS;

d) l'accès aux fonctions de programmation ou de configuration du BPCS peut devoir être limité pour satisfaire les dispositions de gestion des modifications, si le BPCS est combiné avec le SIS.

Dans le cas où une défaillance des équipements communs est susceptible d'entraîner une sollicitation sur le SIS, il conviendrait alors de conduire une analyse pour s'assurer que les taux de danger globaux sont conformes aux prévisions. Le taux de danger global sera la somme du taux des défaillances dangereuses des éléments communs et du taux de danger des autres sources de sollicitation (y compris les défaillances dangereuses des parties indépendantes du SIS).

La séparation entre le SIS et le BPCS peut utiliser une séparation identique ou différente. Une séparation identique signifierait l'utilisation de la même technologie pour le BPCS et pour le SIS, tandis qu'une séparation différente signifierait l'utilisation de technologies différentes, issues d'un même constructeur ou de différents constructeurs.

Comparée à la séparation identique, qui apporte une amélioration vis-à-vis des défaillances aléatoires, la séparation différente offre l'avantage supplémentaire de réduire la probabilité des anomalies systématiques et de réduire les défaillances de cause commune.

La séparation identique entre le SIS et le BPCS peut présenter certains avantages pour la conception et la maintenance, parce qu'elle réduit la vraisemblance des erreurs de maintenance. Ceci est en particulier le cas si différents composants doivent être choisis et qu'ils n'ont pas été utilisés auparavant au sein de l'organisme de l'utilisateur.

La séparation identique entre le SIS et le BPCS peut être acceptable pour des applications de SIL 1, de SIL 2 et de SIL 3, bien que les sources et les effets des défaillances de cause commune doivent être étudiés et leur vraisemblance réduite. Quelques exemples de défaillances de cause commune sont:

a) le raccordement des connexions des instruments et des lignes de sortie d'impulsion;

b) la corrosion et l'érosion;

c) les anomalies de matériel dues à des causes environnementales;

d) les erreurs de logiciel;

e) les alimentations en énergie et les sources de puissance;

f) les erreurs humaines.

La séparation différente offre l'avantage supplémentaire de réduire la probabilité des défaillances systématiques (un facteur particulièrement important dans les applications de SIL 3 et de SIL 4) et de réduire des défaillances de cause commune.

Il y a quatre zones où la séparation entre le SIS et le BPCS est généralement octroyée:

1) les capteurs sur le terrain;

2) les éléments terminaux;

3) l'unité logique;

4) le câblage.

b) To retain flexibility for changes, maintenance , testing and documentation relating to the BPCS.

NOTE 1 The SIS normally has more robust requirements than the BPCS and the intent is not to subject the BPCS to the same robust requirements that are required for the SIS. However it should be noted that uncontrolled BPCS modifications can be a cause of increased demand on the SIS.

c) To facilitate the validation and functional safety assessment of the SIS.

d) Access to the programming or configuration functions of the BPCS may need to be limited to meet the modification management arrangements if the BPCS is combined with the SIS.

Where a failure of the common equipment can cause a demand on the SIS, then an analysis should be conducted to ensure the overall hazard rates satisfies the expectations. The overall hazard rate will be the sum of the dangerous failure rate of the common elements and the hazard rate from other sources of demand (including dangerous failure of the independent parts of the SIS).

Separation between the SIS and the BPCS may use identical or diverse separation. Identical separation would mean using the same technology for both the BPCS and SIS whereas diverse separation would mean using different technologies from the same or different manufacturer.

Compared with identical separation, which helps against random failures, diverse separation offers the additional benefit of reducing the probability of systematic faults and of reducing common cause failures.

Identical separation between the SIS and BPCS may have some advantages in design and maintenance because it reduces the likelihood of maintenance errors. This is particularly the case if diverse components are to be selected which have not been used before within the user's organisation.

Identical separation between SIS and BPCS may be acceptable for SIL 1, SIL 2 and SIL 3 applications although the sources and effects of common cause failures should be considered and their likelihood reduced. Some examples of common cause failures are:

a) plugging of instrument connections and impulse lead lines;

b) corrosion and erosion;

c) hardware faults due to environmental causes;

d) software errors;

e) power supplies and power sources;

f) human errors.

Diverse separation offers the additional benefit of reducing the probability of systematic failures (a factor especially important in SIL 3 and SIL 4 applications) and reducing common cause failures.

There are four areas where separation between the SIS and BPCS is generally provided:

1) field sensors;

2) final elements;

3) logic solver;

4) wiring.

La séparation physique entre le BPCS et le SIS peut ne pas être nécessairement fournie si l'indépendance est maintenue, et si les configurations des équipements et les méthodes appliquées assurent que le SIS ne sera pas dangereusement affecté par:

- les défaillances du BPCS;
- les travaux réalisés sur le BPCS, par exemple, maintenance, exploitation ou modification.

Dans le cas où des procédures seraient nécessaires pour s'assurer que le SIS n'est pas dangereusement affecté, le concepteur du SIS devra indiquer les procédures à appliquer.

a) Capteurs sur le terrain

L'utilisation d'un capteur unique pour le BPCS et pour le SIS demande un examen et une analyse plus approfondis. Un examen et une analyse supplémentaires sont nécessaires parce qu'une défaillance de cet unique capteur pourrait avoir comme conséquence une situation dangereuse. Par exemple, un unique capteur de niveau utilisé à la fois pour le BPCS et pour un déclenchement à niveau haut du SIS pourrait créer une sollicitation si le capteur se bloque (tombe en panne) au niveau bas (c'est-à-dire, au-dessous du point de consigne du contrôleur de niveau). Du fait que le capteur se bloquerait au niveau bas, le contrôleur commanderait l'ouverture de la vanne. Puisque le même capteur est utilisé pour le SIS, il ne détectera pas l'état niveau haut résultant.

Dans le cas où un capteur unique serait utilisé pour un BPCS et une fonction du SIS, les exigences de la CEI 61511 ne seront généralement satisfaites que si les diagnostics relatifs au capteur peuvent réduire suffisamment le taux des défaillances dangereuses et si le SIS est capable de placer le processus dans un état de sécurité, en temps voulu. En pratique, ceci est difficile à réaliser, même pour des applications de SIL 1. Pour une fonction instrumentée de sécurité de SIL 2, de SIL 3 ou de SIL 4, des capteurs séparés au sein du SIS, avec une redondance identique ou différente, seront généralement nécessaires pour obtenir l'intégrité de sécurité requise.

NOTE 2 Lorsqu'un capteur séparé et unique est utilisé pour le SIS, il peut être avantageux de répéter le signal vers le BPCS par l'intermédiaire d'isolateurs/coupleurs ad hoc. Cette configuration peut conduire à améliorer la couverture de diagnostic, en permettant une comparaison de signal entre les capteurs du BPCS et du SIS.

Lorsque des capteurs du SIS redondants sont utilisés, ils peuvent être également reliés au BPCS par des isolateurs/coupleurs ad hoc. Des algorithmes appropriés au sein du BPCS, tel que la «moyenne de trois» peuvent augmenter la sécurité en réduisant le taux de sollicitation sur le SIS.

b) Elément terminal

Comme dans le cas des capteurs, l'utilisation d'une vanne unique pour le BPCS et pour le SIS demande un examen et une analyse plus approfondis. En général, l'utilisation d'une vanne unique pour le SIS et pour le BPCS n'est pas recommandée dans le cas où une défaillance de la vanne peut entraîner une sollicitation sur le SIS.

Dans le cas où une vanne unique serait utilisée à la fois pour le BPCS et pour le SIS, les exigences de la CEI 61511 ne seront généralement satisfaites que si les diagnostics relatifs à la vanne peuvent réduire suffisamment le taux des défaillances dangereuses et si le SIS est capable de placer le processus dans un état de sécurité, en temps voulu.

En pratique, ceci est difficile à réaliser, même pour des applications de SIL 1. Pour une fonction instrumentée de sécurité de SIL 2, de SIL 3 ou de SIL 4, des vannes séparées au sein du SIS, avec une redondance identique ou différente, seront généralement nécessaires pour obtenir l'intégrité de sécurité requise.

Dans le cas où une vanne unique serait utilisée à la fois pour des fonctions du BPCS et du SIS, il conviendrait que la conception garantisse que l'action du SIS soit prioritaire sur l'action du BPCS. Ceci est habituellement réalisé avec le SIS directement connecté à une électrovanne qui coupe la source d'alimentation directement sur l'actionneur, par exemple, entre le positionneur de vanne et l'actionneur.

Lorsque des vannes de SIS redondantes sont utilisées, elles peuvent être connectées à la fois au SIS et au BPCS.

Physical separation between BPCS and SIS may not be necessary provided independence is maintained, and the equipment arrangements and the procedures applied ensure the SIS will not be dangerously affected by

- failures of the BPCS;
- work carried out on the BPCS for example, maintenance, operation or modification.

Where procedures are necessary to ensure the SIS is not dangerously affected, the SIS designer will then need to specify the procedures to be applied.

a) Field sensors

Using a single sensor for both the BPCS and SIS requires further review and analysis. The additional review and analysis is necessary because a failure of this single sensor could result in a hazardous situation. For example, a single level sensor used for both the BPCS and a SIS high level trip could create a demand if the sensor fails low (i.e., below the set point of the level controller). As a result of the sensor failing low, the controller would drive the valve open. Since the same sensor is used for the SIS, then it will not detect the resultant high level condition.

Where a single sensor is used for both a BPCS and SIS function, the requirements of IEC 61511-1 will normally only be satisfied if the sensor diagnostics can reduce the dangerous failure rate sufficiently and the SIS is capable of placing the process in a safe state within the required time. In practice this is difficult to achieve even for SIL 1 applications. For a SIL 2, SIL 3 or SIL 4 safety instrumented function, separate SIS sensors with identical or diverse redundancy will normally be needed to meet the required safety integrity.

NOTE 2 When a single separate SIS sensor is used, there may be advantages to repeating the signal to the BPCS through suitable isolators. Such an arrangement can lead to improved diagnostic coverage by allowing signal comparison between BPCS and SIS sensors.

When redundant SIS sensors are used, the sensors may also be connected to the BPCS through suitable isolators. Suitable algorithms in the BPCS such as “middle of three” may increase safety by reducing the demand rate on the SIS.

b) Final Element

In the same way as for the sensors, using a single valve for both the BPCS and SIS requires further review and analysis. In general, a single valve used for both the SIS and BPCS in not recommended if a failure of the valve would place a demand on the SIS.

Where a single valve is used by both the BPCS and SIS, the requirements of IEC 61511-1 will normally only be satisfied if the valve diagnostics can reduce the dangerous failure rate sufficiently and the SIS is capable of placing the process in a safe state within the required time.

In practice, this is difficult to achieve even for SIL 1 applications. For a SIL 2, SIL 3 or SIL 4 safety instrumented function, separate SIS valves with identical or diverse redundancy will normally be needed to meet the required safety integrity.

Where a single valve is used for both BPCS and SIS functions, the design should ensure that the SIS action overrides the BPCS action. This is normally achieved by having the SIS directly connected to a solenoid valve that removes the power source directly at the actuator, for example, between the valve positioner and the actuator.

When redundant SIS valves are used, the valves may be connected to both the SIS and BPCS.

NOTE 3 Même avec des vannes redondantes, il est important de considérer les défaillances de cause commune entre les vannes du BPCS et du SIS.

Les considérations supplémentaires pour déterminer les exigences des vannes sont:

– les exigences de fermeture;
– l'expérience de fiabilité avec la vanne dans les applications de processus similaires;
– les modes de défaillance dangereux de la vanne;
– les procédures opérationnelles qui rendent la vanne moins efficace (par exemple, des vannes de dérivation ouvertes);
– les exigences des tests périodiques.

c) Câblage

Sur les systèmes «activer pour déclencher», le BPCS et le câblage relatif aux dispositifs de terrain sont généralement séparés du câblage allant au SIS et à ses dispositifs de terrain concernés en raison de la possibilité de désactiver accidentellement la fonction de sécurité, sans avis préalable. Les directives habituelles pour ces types de systèmes comprennent l'installation de câbles multi-conducteurs séparés et de boîtes de jonction dédiées au SIS et au BPCS. Dans le cas où le câblage ne serait pas séparé, nous suggérons alors d'utiliser de bonnes procédures de marquage et de maintenance pour réduire au minimum les erreurs potentielles provoquées pendant la maintenance et ayant pour résultat la désactivation du SIS.

NOTE 4 «Activer pour déclencher» se rapporte à des circuits de la SIF pour lesquels les sorties et les dispositifs sont désactivés en exploitation normale. L'application de l'énergie (par exemple, électricité, air) entraîne une action de déclenchement.

Le système de support de câble (par exemple, chemins de câbles, conduits), peut être commun à la fois aux systèmes «désactiver pour déclencher» et «activer pour déclencher», sauf si la séparation est requise pour d'autres raisons (par exemple, interférences électromagnétiques). Sur les systèmes «activer pour déclencher», une adjonction de protection contre l'incendie des chemins de câbles peut être étudiée dans des zones à risque d'incendie.

11.2.5 Aucune ligne directrice n'est fournie.

11.2.6 Voir le Paragraphe 11.8 de la présente partie pour des directives, ainsi que les lignes directrices suivantes concernant la note du Paragraphe 11.2.5 de la CEI 61511-1.

Les opérateurs, le personnel de maintenance, les superviseurs et les directeurs ont tous des rôles à jouer dans l'exploitation sûre de l'installation industrielle. Cependant, l'homme peut faire des erreurs ou peut être incapable d'accomplir une tâche, tout comme les instruments et les équipements peuvent être sujets à des dysfonctionnements ou à des défaillances.

Les performances humaines constituent donc un élément de conception du système. L'interface homme-machine (HMI) est particulièrement importante lors du dialogue relatif à l'état du SIS vis-à-vis du personnel d'exploitation et de maintenance.

L'analyse de fiabilité humaine (HRA) identifie les conditions qui font que des personnes commettent des erreurs et fournit des évaluations de taux d'erreurs basées sur des statistiques antérieures et sur des études comportementales. Quelques exemples d'erreurs humaines contribuant au risque sécuritaire d'un processus chimique sont données ci-après:

– des erreurs non détectées à la conception;
– des erreurs en exploitation (par exemple, faux point de consigne);
– une maintenance impropre (par exemple, remplacement d'une vanne par une autre ayant un comportement incorrect lors d'une défaillance);
– des erreurs d'étalonnage, d'essai ou d'interprétation de sortie de systèmes de commande;
– le refus de répondre correctement à une urgence.

NOTE 3 Even with redundant valves, it is important to consider common cause failures between the BPCS and SIS valves.

Additional considerations for determining the valve requirements are:

– shutoff requirements;
– reliability experience with the valve in similar process applications;
– unsafe failure modes of the valve;
– operating procedures that make the valve less effective (for example, bypass valves being opened);
– proof testing requirements.

c) Wiring

On energize to trip systems, the BPCS and relevant field device wiring is normally separated from wiring to the SIS and its relevant field devices because of the possibility of accidentally deactivating the safety function without noticing it. Typical guidelines for these types of systems include installing separate multi-conductor cables and junction boxes dedicated to the SIS and BPCS. Where the wiring is not separated, the use of good labelling and maintenance procedures to minimize the potential of errors caused during maintenance resulting in deactivation of the SIS are suggested.

NOTE Energize to trip refers to SIF circuits where the outputs and devices are de-energized under normal operation. Application of power (for example, electricity, air) causes a trip action.

The cable support system (for example, cable trays, conduit), may be common for both de-energize to trip and energize to trip systems, unless separation is required for other reasons (for example, electromagnetic interference). On energize to trip systems, consideration may be given to adding fire protection to the cable trays in fire risk areas.

11.2.5 No further guidance provided.

11.2.6 See 11.8 of this standard for guidance as well as following guidance relating to the Note in 11.2.5 of IEC 61511-1.

The operators, maintenance staff, supervisors and managers all have roles in safe plant operation. However, humans can make errors or be unable to perform a task, just as instruments and equipment are subject to malfunction or failure.

Human performance is therefore a system design element. The human machine interface (HMI) is particularly important in communicating the status of the SIS to operating and maintenance personnel.

Human Reliability Analysis (HRA) identifies conditions that cause people to err and provides estimates of error rates based on past statistics and behavioural studies. Some examples of human error contributing to chemical process safety risk include:

- undetected errors in design;
- errors in operations (for example, wrong set point);
- improper maintenance (for example, replacing a valve with one having the incorrect failure action);
- errors in calibrating, testing or interpreting output from control systems;
- failure to respond properly to an emergency.

NOTE Voyez les références suivantes pour des directives supplémentaires:

CCPS/AIChE *Directives relatives aux performances humaines améliorées dans la sécurité des processus*, New York: American Institute of Chemical Engineers (1994).
CCPS/AIChE *Directives relatives à l'analyse de risque quantitative des processus chimiques*, New York: American Institute of Chemical Engineers (2000).

HSE *Réduction des erreurs et comportement d'influence*, HSG48, Health & Safety Executive, London (1999), ISBN 0 7176 2452 8

11.2.7 Ce paragraphe concerne le danger potentiel susceptible d'être généré en cas de redémarrage automatique du processus par un SIS immédiatement après correction de la condition de déclenchement. Il convient que chaque SIF soit analysée pour déterminer comment il devrait être réinitialisé une fois que la condition de déclenchement a été corrigée. Généralement, il convient que le redémarrage ne soit possible qu'après une action manuelle de l'opérateur.

11.2.8 Des moyens manuels indépendants à la fois de l'unité logique du SIS et du système de commande du BPCS peuvent être fournis pour permettre à l'opérateur de lancer un arrêt en cas d'urgence. Les exigences pour l'arrêt manuel sont habituellement définies dans la SRS.

L'arrêt d'urgence peut être connecté à l'unité logique à électronique programmable (PE) du SIS (par exemple, lorsqu'un arrêt en séquence est demandé) à condition qu'il soit nécessaire et considéré comme approprié par l'équipe de H&RA.

11.2.9 Ce paragraphe indique le besoin d'analyser l'indépendance entre le SIS et les autres couches de protection et pas simplement entre le SIS et le BPCS (voir la CEI 61511-1, Figure 9).

Dans certaines circonstances, il peut être acceptable d'avoir une séparation partielle entre le BPCS et le SIS. Ceci est en particulier le cas lorsqu'une défaillance des équipements communs ne provoquera pas de sollicitation sur le SIS. Dans ce cas, il est nécessaire de mettre en oeuvre des équipements communs ou partagés, en accord avec la CEI 61511-1.

Dans le cas où une défaillance des équipements communs est susceptible d'entraîner une sollicitation sur le SIS, il convient alors de conduire une analyse pour s'assurer que le taux de danger global est conforme aux prévisions. Le taux de danger global sera la somme du taux des défaillances dangereuses des éléments communs et du taux de danger des autres sources de sollicitation (y compris les défaillances dangereuses des parties indépendantes du SIS). Pour définir les dangers associés aux défaillances dangereuses des équipements communs, il convient de considérer les cas suivants.

a) Lorsqu'un élément de la configuration redondant est utilisé comme BPCS, il faut considérer les dangers résultant des défaillances dangereuses des équipements communs, en prenant en compte les performances du SIS, qui a été dégradé par les instruments défaillants;

c) Lorsque les instruments partagés ne sont pas redondants, il faut considérer les dangers résultant des défaillances dangereuses des équipements communs, en supposant que le SIS n'a pas répondu.

11.2.10 Donne des directives d'avertissement sur utilisation d'un élément commun pour le BPCS et le SIS. Le terme «suffisamment bas» dans la note signifie que le taux des défaillances dangereuses des équipements partagés, multiplié par la PFD des autres de couches indépendantes (autre que la SIF), satisfait aux critères de risque d'entreprise.

11.2.11 Dans le cas des éléments terminaux, qui sur une perte d'alimentation, ne conduisent pas à l'état de sécurité (par exemple, systèmes «activer pour déclencher»), il convient d'attirer l'attention sur la mise à disposition de moyens manuels locaux pour obtenir l'état de sécurité.

NOTE See the following references for additional guidance:

CCPS/AIChE *Guidelines for Improved Human Performance in Process Safety*, New York: American Institute of Chemical Engineers (1994).

CCPS/AIChE *Guidelines for Chemical Process Quantitative Risk Analysis* (second edition), New York: American Institute of Chemical Engineers (2000).

HSE *Reducing error and influencing behaviour*, HSG48, Health and Safety Executive, London (1999), ISBN 0 7176 2452 8.

11.2.7 This subclause addresses the potential hazard that may be created if a SIS automatically restarts the process immediately after the trip condition is corrected. Each SIF should be analysed to determine how it should be reset once the trip condition is corrected. Normally restarting should only be possible after a manual action of the operator.

11.2.8 Manual means that are independent of both the SIS logic solver and the BPCS control system may be provided to allow the operator to initiate a shutdown in an emergency. The requirements for manual shutdown are normally defined in the SRS.

The emergency stop may be connected to the SIS PE logic solver (for example, when a sequenced shut down is required) provided that it is necessary and deemed appropriate by the H and RA team.

11.2.9 This subclause indicates the need for analysis of independence between the SIS and other protection layers, not just between the SIS and BPCS (see IEC 61511-1, Figure 9).

Under some circumstances it may be acceptable that there is incomplete separation between BPCS and the SIS. This is particularly the case where a failure of the common equipment will not cause a demand on the SIS. In such cases, it is necessary to implement the common or shared equipment in accordance with IEC 61511-1.

Where a failure of the common equipment can cause a demand on the SIS, then an analysis should be conducted to ensure the overall hazard rate satisfies the expectations. The overall hazard rate will be the sum of the dangerous failure rate of the common elements and the hazard rate from other sources of demand (including dangerous failure of the independent parts of the SIS). To establish the hazards associated with dangerous failures of the common equipment, the following cases should be considered:

a) Where one element of the redundant configuration is used as a BPCS, consider the hazards arising from dangerous failures of common equipment taking into consideration the performance of the SIS which has been degraded by the failed instruments;

b) Where the shared instruments are not redundant, consider the hazards arising from dangerous failures of the common equipment assuming the SIS did not respond.

11.2.10 Provides cautionary guidelines on using a common element for both the BPCS and the SIS. “Sufficiently low” in the Note means the dangerous failure rate of the shared equipment multiplied by the PFD of the other independent layers (other than the SIF) meets your corporate risk criteria.

11.2.11 In the case of final elements which on loss of power do not fail to the safe state (for example, energize to trip systems) consideration should be given to the provision of local manual means to achieve the safe state.

11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie

11.3.1 Aucune ligne directrice n'est fournie.

11.3.2 Aucune ligne directrice n'est fournie.

11.3.3 Aucune ligne directrice n'est fournie.

11.4 Exigences relatives à la tolérance aux anomalies du matériel

11.4.1 L'approche traditionnelle vis-à-vis de la conception d'un système de sécurité était de s'assurer qu'aucune anomalie isolée n'aurait comme conséquence la perte de la fonction prévue. Les architectures de système telles que 1oo2 ou 2oo3 ont une tolérance aux anomalies de type 1, parce qu'elles peuvent fonctionner sur sollicitation, même en présence d'une anomalie dangereuse. Ces systèmes ont été utilisés comme approche normalisée pour les systèmes de sécurité, afin de s'assurer qu'ils étaient suffisamment robustes pour pouvoir résister à des défaillances aléatoires du matériel. Les architectures à tolérance aux anomalies ont également apporté une protection pour une large gamme d'anomalies systématiques (principalement dans le matériel), parce que ces dernières ne se présentent pas nécessairement au même moment dans le temps.

Cette norme admet que la production industrielle par processus a besoin de plusieurs niveaux de performances des systèmes de sécurité et elle a adopté le concept des niveaux d'intégrité de sécurité avec des performances croissantes, en fonction du besoin de réduction de risque de l'application spécifique impliquée. En raison des différents niveaux de performances, il n'est plus pertinent de s'attendre à ce que tous les niveaux d'intégrité de sécurité soient tolérants aux anomalies. En choisissant l'architecture pour utiliser un niveau spécifié d'intégrité, il est cependant important de s'assurer qu'il est suffisamment robuste pour les anomalies aléatoires du matériel et les anomalies systématiques. Pour assurer la robustesse vis-à-vis des anomalies aléatoires du matériel, cette norme demande qu'une analyse de fiabilité soit effectuée.

Les exigences de cette partie de la norme sont ciblées pour s'assurer que les architectures ont la tolérance aux anomalies nécessaire, pour les anomalies aléatoires du matériel et certaines anomalies systématiques. En décidant de l'étendue de la tolérance aux anomalies nécessaire, il convient de prendre en compte un certain nombre de facteurs, indiqués ci-après:

– la complexité des dispositifs utilisés au sein du sous-système. Un dispositif sera moins susceptible d'être sujet à des anomalies systématiques si les modes de défaillance sont bien définis, le comportement dans des conditions d'anomalie peut être déterminé, et on dispose de données de défaillance suffisantes provenant de l'expérience sur le terrain;

– dans quelle mesure les anomalies conduisent à un état de sécurité ou peuvent être détectées par des diagnostics, de manière à ce qu'une action spécifiée puisse être prise. Cette possibilité est nommée la «proportion de défaillances en sécurité» du dispositif;

– l'exigence du niveau d'intégrité de sécurité pour l'application impliquée.

Le groupe de travail international qui a préparé la CEI 61508 a considéré les facteurs ci-dessus et a spécifié l'étendue de la tolérance aux anomalies nécessaire, dans la CEI 61508-2. En préparant cette norme sectorielle spécifique pour le domaine des processus, il a été considéré que les exigences pour la tolérance aux anomalies des dispositifs de terrain et unités logiques à électronique non programmable (non-PE), pourraient être simplifiées et que les exigences de la CEI 61511-1 pourraient être appliquées en tant qu'alternative. Il convient de noter qu'afin de satisfaire aux exigences de disponibilité, les conceptions de sous-systèmes peuvent nécessiter plus de redondance de composants que ce qui est mentionné dans les Tableaux 5 et 6.

11.3 Requirements for system behaviour on detection of a fault

11.3.1 No further guidance provided.

11.3.2 No further guidance provided.

11.3.3 No further guidance provided.

11.4 Requirements for hardware fault tolerance

11.4.1 The traditional approach to safety system design was to ensure that no single fault would result in loss of intended function. System architectures such as 1oo2 or 2oo3 have a fault tolerance of 1 because they are able to function on demand even in the presence of one dangerous fault. Such systems were employed as a standard approach for safety systems to ensure they were sufficiently robust to be able to withstand random hardware failures. Fault tolerance architectures also gave protection to a wide range of systematic faults (mainly in hardware) because such faults do not necessarily arise at the same instant of time.

This standard recognizes that the process industry needs more than one level of performance from safety systems and has adopted the concept of safety integrity levels with increasing performance depending on the need for risk reduction in the specific application involved. Because of the different levels of performance it is no longer appropriate to expect all safety integrity levels to be fault tolerant. In selecting the architecture to use for a specified integrity level it is however important to ensure that it is sufficiently robust for both random hardware faults and systematic faults. To ensure robustness against random hardware faults this standard requires that a reliability analysis be carried out.

The requirements of this part of the standard are targeted at ensuring that architectures have the necessary fault tolerance for random hardware faults and some systematic faults. In deciding the extent of fault tolerance needed there are a number of factors that should be taken into consideration as follows:

- The complexity of the devices used within the subsystem. A device will be less likely to be subject to systematic faults if the failure modes are well defined, the behaviour under fault conditions can be determined and there is sufficient failure data from field experience;
- The extent to which faults lead to a safe condition or can be detected by diagnostics so that a specified action can be taken. This capability is termed the safe failure fraction of the device;
- The safety integrity level requirement for the application involved.

The international working group that prepared IEC 61508 considered the above factors and specified the extent of fault tolerance required in IEC 61508-2. In preparing this sector-specific standard for the process sector it was considered that the requirements for fault tolerance of field devices and non PE logic solver could be simplified and the requirements in IEC 61511-1 could be applied as an alternative. It should be noted that subsystem designs may require more component redundancy than what is stated in Tables 5 and 6 in order to satisfy availability requirements.

Les exigences relatives à la tolérance aux anomalies du matériel peuvent s'appliquer à des composants individuels ou à des sous-systèmes, nécessaires pour exécuter une SIF. Par exemple, dans le cas d'un sous-système de capteurs comprenant un certain nombre de capteurs redondants, l'exigence de tolérance aux anomalies s'applique au sous-système de capteurs dans son ensemble et non pas aux capteurs individuels.

11.4.2 Le Tableau 5 de la CEI 61511-1 définit la tolérance minimale aux anomalies pour les unités logiques à électronique programmable (PE). La prescription de tolérance aux anomalies dépend du SIL requis du SIS et de la portion de défaillances en sécurité du sous-système. Les informations sur la portion de défaillances en sécurité des unités logiques peuvent généralement être obtenues du fournisseur de l'unité logique à électronique programmable (PE). Si l'unité logique à électronique programmable (PE) n'est pas utilisée selon les hypothèses faites lors du calcul de la SFF, il convient alors que les déclarations faites pour la portion de défaillances en sécurité soient soigneusement considérées. En particulier, il convient que les hypothèses faites soient examinées, pour s'assurer que la frontière et l'environnement supposés dans les calculs de la SFF sont valides pour l'application considérée. Cela est dû au fait que la SFF dépendra d'un certain nombre de questions telle que: le sous-système est-il activé ou est-il désactivé pour se déclencher? Il convient que les sources de données et les hypothèses faites lors du calcul de la SFF soient documentées. La SFF n'est liée qu'aux défaillances aléatoires du matériel. En établissant la SFF, il est acceptable de supposer que le sous-système a été correctement choisi pour l'application et est installé de manière adéquate, mis en service et maintenu de telle sorte que les défaillances de jeunesse et de fin de vie puissent être exclues de l'évaluation. Il n'est pas nécessaire de considérer les facteurs humains en déterminant la SFF.

11.4.3 Le Tableau 6 de la CEI 61511-1 définit le niveau de base de la tolérance aux anomalies pour les capteurs, les éléments terminaux, et les unités logiques non-PE, en ayant la limite de revendication du SIL requise dans la première colonne. Les exigences du Tableau 6 sont basées sur les exigences de la CEI 61508-2, pour des dispositifs à électronique programmable (PE), avec une SFF entre 60 % et 90 %. Les exigences sont fondées sur l'hypothèse que le mode de défaillance dominant est à l'état de sécurité ou bien les défaillances dangereuses sont détectées.

11.4.4 Ce paragraphe permet, dans certaines conditions, de diminuer d'une unité la tolérance aux anomalies du matériel de tous les sous-systèmes, excepté les unités logiques à électronique programmable (PE). Ces conditions s'appliqueront aux dispositifs tels que les vannes ou les transmetteurs intelligents et réduiront la vraisemblance des défaillances systématiques, de telle manière que les exigences soient alignées sur celles de la CEI 61508-2, pour les dispositifs non-PE.

11.4.5 Dans certains cas, il peut être possible de réduire la tolérance aux anomalies, en suivant les exigences de tolérance aux anomalies de la CEI 61508-2. Ceci peut être réalisé en introduisant des diagnostics supplémentaires, tels que la comparaison de signal ou des essais de course partielle régulièrement programmés, de telle manière que la SFF des sous-systèmes soit supérieure à 90 %.

11.5 Exigences relatives au choix des composants et des sous-systèmes

11.5.1 Objectifs

Aucune ligne directrice n'est fournie.

The requirements for hardware fault tolerance can apply to individual components or subsystems required to perform a SIF. For example, in the case of a sensor subsystem comprising a number of redundant sensors, the fault tolerance requirement applies to the sensor subsystem in total, not to individual sensors.

11.4.2 Table 5 of IEC 61511-1 defines the minimum fault tolerance for PE logic solvers. The fault tolerance requirement depends on the required SIL of the SIS and the subsystem safe failure fraction. Information on safe failure fraction of logic solvers can normally be obtained from the PE logic solver vendor. If the PE logic solver is not used according to the assumptions made in the calculation of the SFF then the claims made for safe failure fraction should be carefully considered. In particular, the assumptions made should be examined to ensure that the boundary and environment assumed in the SFF calculations are valid for the application being considered. This is because the SFF will depend on a number of issues such as whether the subsystem is energize or de-energize to trip. Data sources and assumptions made during a calculation of SFF should be documented. The SFF is related to random hardware failures only. In establishing the SFF it is acceptable to assume that the subsystem has been properly selected for the application and is adequately installed, commissioned and maintained such that early life failures and age related failure may be excluded from the assessment. Human factors do not need to be considered when determining SFF.

11.4.3 Table 6 of IEC 61511-1 defines the basic level of fault tolerance for sensors, final elements, and non-PE logic solvers having the required SIL claim limit in the first column. The requirements in Table 6 are based on the requirements in IEC 61508-2 for PE devices with a SFF between 60 and 90 %. The requirements are based on the assumption that the dominant failure mode is to the safe state or that dangerous failures are detected.

11.4.4 This subclause allows the hardware fault tolerance of all subsystems except PE logic solvers to be reduced by one on certain conditions. These conditions will apply to devices such as valves or smart transmitters and reduce the likelihood of systematic failures such that the requirements are aligned to the requirements of IEC 61508-2 for non PE devices.

11.4.5 In some cases it may be possible to reduce the fault tolerance by following the fault tolerance requirements of IEC 61508-2. This may be achieved by introducing additional diagnostics such as signal comparison or regularly scheduled partial stroke testing such that the SFF of the subsystems is higher than 90 %.

11.5 Requirements for selection of components and subsystems

11.5.1 Objectives

No further guidance provided.

11.5.2 Exigences générales

11.5.2.1 Certaines considérations sont à prendre en compte pour choisir les composants et les sous-systèmes à utiliser au sein d'un SIS. La première option est relative à la conformité des composants par rapport à la CEI 61508-2 et à la CEI 61508-3 . La deuxième option est relative à l'utilisation de composants et de sous-systèmes reconnus comme étant fiables du fait d'une utilisation intensive dans des conditions de service similaires et dans un environnement semblable.

Quelle que soit l'option choisie, il doit être démontré que le composant ou le sous-système

a) est assez fiable pour atteindre la PFD cible globale ou le taux cible des défaillances dangereuses de la fonction instrumentée de sécurité,

b) satisfait à l'exigence de contrainte architecturale et

c) présente une vraisemblance d'anomalies systématiques suffisamment faible.

La prescription du point c) peut être satisfaite, soit par la conformité aux Parties 2 et 3 de la CEI 61508, soit par une utilisation préalable des exigences du paragraphe 11.5 de la présente norme.

11.5.2.2 Aucune ligne directrice n'est fournie.

11.5.2.3 Aucune ligne directrice n'est fournie.

11.5.2.4 Aucune ligne directrice n'est fournie.

11.5.3 Exigences relatives au choix des composants et des sous-systèmes basés sur une utilisation antérieure

11.5.3.1 Il y a très peu de dispositifs de terrain (capteurs et vannes) conçus suivant la CEI 61508-2 et la CEI 61508-3. Les utilisateurs et les concepteurs dépendront donc plus étroitement de l'utilisation de dispositifs de terrain qui ont été «validés en utilisation».

De nombreux utilisateurs ont une liste d'instruments approuvés ou recommandés pour utilisation dans leur installation. Ces listes ont été établies sur la base d'une large expérience de fonctionnement satisfaisant sur leur BPCS. Les capteurs et les vannes qui ont eu un historique de performances non satisfaisantes ont été éliminés.

Généralement les capteurs et les vannes qui figurent sur ces listes d'instruments approuvés ou recommandés pour le BPCS, pourraient également être considérés comme «validés en utilisation» pour les SIS soumis à l'évaluation requise par la CEI 61511-1. Il convient que cette liste d'instruments comprenne la version du dispositif et qu'elle soit complétée par un contrôle documenté des retours du terrain au niveau de l'utilisateur et au niveau du fabricant. De plus, il convient que le fabricant dispose d'un système de modification incorporant l'évaluation de l'impact des défaillances rapportées et des modifications introduites.

Si une telle liste n'existe pas, les utilisateurs et les concepteurs doivent alors conduire une évaluation sur les capteurs et les vannes pour s'assurer qu'ils sont satisfaisants et que l'instrument fonctionnera comme cela est souhaité. Ceci peut exiger des discussions avec d'autres utilisateurs ou concepteurs pour voir ce qu'ils utilisent pour des applications similaires.

11.5.3.2 Il convient de noter que pour des dispositifs plus complexes, il peut devenir plus difficile de montrer que l'expérience acquise dans une application est pertinente. Par exemple, une expérience acquise par l'utilisation d'un PLC dans une application impliquant l'emploi d'un langage ladder simple, peut ne pas être appropriée à une utilisation de l'équipement pour des calculs ou des séquences complexes.

11.5.2 General requirements

11.5.2.1 There are some considerations for selecting components and sub–systems to be used in a SIS. The first option is that the components be designed in accordance with IEC 61508–2 (requirements for electrical/electronic/programmable electronic safety-related systems) and IEC 61508-3 (software requirements). The second option is to use components and sub–systems that are known to be reliable through extensive use in similar service and in a similar environment.

Whichever option is chosen, it has to be demonstrated that the component or subsystem

a) is reliable enough to achieve the overall target PFD or target dangerous failure rate of the safety instrumented function,

b) meets the architectural constraint requirement, and

c) has a sufficiently low likelihood of systematic faults.

The requirement of c) can be satisfied either by compliance with IEC 61508-2 and IEC 61508-3 or by the prior use requirements in 11.5 of this standard.

11.5.2.2 No further guidance provided.

11.5.2.3 No further guidance provided.

11.5.2.4 No further guidance provided.

11.5.3 Requirements for the selection of components and subsystems based on prior use

11.5.3.1 There are very few field devices (sensors and valves) that are designed per IEC 61508-2 and IEC 61508-3. Users and designers will therefore have to depend more heavily on using field devices that have been “proven-in-use”.

Many users have a list of instruments that are approved or recommended for use in their facility. These lists have been established by extensive successful operating experience on their BPCS. Sensors and valves that have had a history of not performing as desired have been eliminated.

Normally the sensors and valves that are on these approved or recommended lists for the BPCS could also be considered as proven-in-use for SISs subject to the assessment required by 61511-1. This list of instruments should include the version of the device and be supported by documented monitoring of field returns at the user and at the manufacturer. In addition the manufacturer should have a modification process which evaluates the impact of reported failures and modifications.

If such a list does not exist, then users and designers need to conduct an assessment on the sensors and valves to ensure that they are satisfied the instrument will perform as desired. This may require discussions with other users or designers to see what they are using for similar applications.

11.5.3.2 It should be noted that for more complex devices, it may become more difficult to show that the experience gained in an application is relevant. As an example, experience gained by using a PLC in an application involving the use of simple ladder logic may not be relevant if the equipment was to be used for complex calculations or sequences.

En général, les aspects concernés relatifs au profil de fonctionnement des dispositifs de terrain sont différents de ceux d'une unité logique.

Pour les dispositifs de terrain, les points suivants contribuent au profil de fonctionnement:

– la fonctionnalité (par exemple, mesurage, action);
– la plage de fonctionnement;
– les propriétés/caractéristiques du processus (par exemple, propriétés des produits chimiques, de la température, de la pression);
– la connexion au processus.

Pour les unités logiques, les points suivants contribuent au profil de fonctionnement:

– la version et l'architecture du matériel;
– la version et la configuration du logiciel système;
– les logiciels d'application;
– la configuration des E/S;
– le temps de réponse;
– le taux de sollicitation du processus.

Pour tous les dispositifs, les points suivants contribuent au profil de fonctionnement:

– la CEM;
– les conditions d'environnement.

11.5.4 Exigences relatives au choix des composants programmables FPL et des sous-systèmes (par exemple, dispositifs de terrain) basés sur une utilisation antérieure

11.5.4.1 Aucune ligne directrice n'est fournie.

11.5.4.2 Aucune ligne directrice n'est fournie.

11.5.4.3 Aucune ligne directrice n'est fournie.

11.5.4.4 Ce paragraphe explicite des exigences supplémentaires lors de l'essai de qualification d'un dispositif programmable FPL, pour obtenir une capacité SIL 3.

11.5.4.5 Ce paragraphe requiert un manuel de sécurité pour un dispositif programmable FPL avec une capacité SIL 3.

11.5.5 Exigences relatives au choix des composants programmables LVL et des sous-systèmes (par exemple, unités logiques) basés sur une utilisation antérieure

11.5.5.1 Ce paragraphe énumère les exigences supplémentaires concernant les unités logiques à électronique programmable (PE) de LVL, ayant des capacités SIL 1 ou SIL 2. Il convient que l'unité logique à électronique programmable (PE) de LVL avec des capacités SIL 3 ou 4 soit conforme à la CEI 61508-2 et à la CEI 61508-3.

11.5.5.2 Aucune ligne directrice n'est fournie.

11.5.5.3 Aucune ligne directrice n'est fournie.

11.5.5.4 Aucune ligne directrice n'est fournie.

In general, the relevant aspects of the operating profile of field devices are different from those of a logic solver.

For field devices the following points contribute to the operating profile:

- functionality (for example, measurement, action);
- operating range;
- process properties (for example, properties of chemicals, temperature, pressure);
- process connection.

For logic solvers, the following points contribute to the operating profile:

- version and architecture of hardware;
- version and configuration of system software;
- application software;
- I/O configuration;
- response time;
- process demand rate.

For all devices, the following points contribute to the operating profile:

- EMC;
- environmental conditions.

11.5.4 Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use

11.5.4.1 No further guidance provided.

11.5.4.2 No further guidance provided.

11.5.4.3 No further guidance provided.

11.5.4.4 This subclause explains additional requirements when trying to qualify a FPL programmable device to a SIL 3 capability.

11.5.4.5 This subclause mandates a Safety Manual for a FPL programmable device with a SIL 3 capability.

11.5.5 Requirements for the selection of LVL programmable components and subsystems (for example, logic solvers) based on prior use

11.5.5.1 This subclause lists additional requirements for LVL PE logic solvers having SIL 1 or SIL 2 capability. LVL PE logic solver with SIL 3 or 4 capability should be in accordance with IEC 61508-2 and IEC 61508-3.

11.5.5.2 No further guidance provided.

11.5.5.3 No further guidance provided.

11.5.5.4 No further guidance provided.

11.5.5.5 Ce paragraphe énumère les prescriptions supplémentaires pour obtenir les capacités SIL 1 et SIL 2, relatives une unité logique à électronique programmable (PE) configurée pour la sécurité. Pour des considérations supplémentaires, voir l'Annexe D.

11.5.5.6 Ce paragraphe énumère les prescriptions supplémentaires pour obtenir la capacité SIL 2, relatives à une unité logique à électronique programmable (PE) configurée pour la sécurité.

11.5.5.7 Ce paragraphe requiert un manuel de sécurité pour un dispositif programmable LVL avec une capacité SIL 2.

11.5.6 Exigences relatives au choix des composants programmables FVL et des sous-systèmes (par exemple, unités logiques)

11.5.6.1 Aucune ligne directrice n'est fournie.

11.6 Dispositifs de terrain

11.6.1 Aucune ligne directrice n'est fournie.

11.6.2 Aucune ligne directrice n'est fournie.

11.6.3 Aucune ligne directrice n'est fournie.

11.6.4 Aucune ligne directrice n'est fournie.

11.7 Interfaces

Les interfaces d'utilisateur relatives à un SIS sont des interfaces opérateur et des interfaces de maintenance/ingénierie. Les informations ou les données qui sont transmises entre le SIS et les affichages opérateur peuvent être soit relatives au SIS, soit être informatives.

Si une action de l'opérateur fait partie de la fonction instrumentée de sécurité, il convient de considérer tout ce qui est nécessaire pour effectuer cette action comme faisant partie de la SIF. Ceci inclurait, par exemple, une alarme indiquant que l'opérateur doit arrêter le processus. Dans cet exemple, il convient que l'interrupteur d'arrêt (les moyens de mettre en oeuvre l'action d'arrêt) soit considéré comme faisant partie de la SIF.

La transmission des données, qui ne fait pas partie de la SIF (par exemple, l'affichage de la valeur réelle d'un capteur du SIF, si la fonction de déclenchement est réalisée au sein de la SIF) peut être affichée dans le BPCS, s'il peut être mis en évidence que les fonctions instrumentées de sécurité ne sont pas compromises (par exemple, accès à lecture seule dans le BPCS).

11.7.1 Exigences relatives à l'interface opérateur

Les interfaces opérateur utilisées pour transmettre les informations entre l'opérateur et le SIS peuvent inclure

– des afficheurs vidéo;
– des panneaux contenant des lampes/voyants, des boutons-poussoirs et des interrupteurs/commutateurs;
– des dispositifs d'avertissement (visuels et sonores);
– des imprimantes (qui ne devrait pas être la seule méthode de communication);
– toute combinaison de ces derniers.

11.5.5.5 This subclause lists additional requirements to achieve SIL 1 and SIL 2 capability for a safety configured PE logic solver. For additional considerations, see Annex D.

11.5.5.6 This subclause lists additional requirements to achieve SIL 2 capability for a safety configured PE logic solver.

11.5.5.7 This subclause mandates a Safety Manual for a LVL programmable device with a SIL 2 capability.

11.5.6 Requirements for the selection of FVL programmable components and subsystems (for example, logic solvers)

11.5.6.1 No further guidance provided.

11.6 Field devices

11.6.1 No further guidance provided.

11.6.2 No further guidance provided.

11.6.3 No further guidance provided.

11.6.4 No further guidance provided.

11.7 Interfaces

User interfaces to a SIS are operator interfaces and maintenance/engineering interfaces. The information or data which is communicated between the SIS and the operator displays can be either SIS related or informative.

If an operator action is part of the safety instrumented function, everything needed to perform this action should be considered as part of the SIF. This would include, for example, an alarm indicating that the operator has to shutdown the process. In this example, the shutdown switch (the means of implementing the shutdown action) should be considered as part of the SIF.

Data communication which is not part of the SIF (for example, display of the actual value of a SIF sensor if the trip function is realised within the SIF) may be displayed in the BPCS if it can be shown that the safety instrumented functions are not compromised (for example, read-only-access in the BPCS).

11.7.1 Operator interface requirements

The operator interfaces used to communicate information between the operator and the SIS may include:

- video displays;
- panels containing lamps, push buttons, and switches;
- annunciator (visual and audible);
- printers (should not be the sole method of communication);
- any combination of these.

a) Afficheurs vidéo

Les afficheurs vidéo du BPCS peuvent partager les fonctions du SIS et du BPCS à condition que les données affichées soient seulement pour information. Les informations critiques de sécurité sont en plus affichées par l'intermédiaire du SIS (par exemple, si l'opérateur fait partie de la fonction de sécurité).

Lorsqu'une action de l'opérateur est nécessaire pendant des conditions d'urgence, il convient que la mise à jour et les taux de rafraîchissement de l'affichage de l'opérateur soient en accord avec la spécification des exigences concernant la sécurité.

Il convient que les afficheurs vidéo relatifs au SIS soient clairement identifiés en tant que tels, évitant toute ambiguïté ou possibilité de confusion pour l'opérateur, en cas de situation d'urgence.

L'interface opérateur du BPCS peut être utilisée pour offrir une journalisation automatique des événements des fonctions instrumentées de sécurité et des fonctions d'alarme du BPCS.

Les points à consigner pourraient être les suivants:

– les événements du SIS (tels que des occurrences de déclenchement et de pré-déclenchement);

– toutes les fois que l'on a accès au SIS pour des modifications de programme;

– les diagnostics (par exemple, divergences/écarts, etc.).

Il est important que l'opérateur soit alerté lors de la dérivation d'une partie quelconque du SIS, par l'intermédiaire d'une alarme et/ou d'une procédure opérationnelle. Par exemple, la dérivation de l'élément terminal dans un SIS (par exemple, robinet de sectionnement) pourrait être détectée par l'intermédiaire d'interrupteurs de fin de course sur la vanne de dérivation qui activent une alarme sur le tableau de contrôle, ou en installant des blocages ou des verrouillages mécaniques sur la vanne de dérivation qui sont gérés par les procédures opérationnelles. Il est généralement suggéré de maintenir ces alarmes de dérivation distinctes du BPCS.

b) Panneaux

Il convient que les panneaux soient placés en des endroits permettant un accès facile aux opérateurs.

Il convient que les panneaux soient agencés de manière à s'assurer que la disposition des boutons-poussoirs, des lampes/voyants, des instruments de mesurage et de toutes les autres informations ne soit pas susceptible d'être une source de confusion pour l'opérateur. Les interrupteurs d'arrêt pour les différentes unités de processus ou d'équipement qui semblent identiques et qui sont regroupés peuvent avoir comme conséquence l'arrêt intempestif d'un équipement par un opérateur stressé par une situation d'urgence. Il convient que les interrupteurs d'arrêt soient physiquement séparés et que leur fonction soit identifiée par une étiquette. Il convient de donner des moyens pour essayer toutes les lampes/voyants.

c) Imprimantes et journalisation

Il convient que les imprimantes connectées au SIS ne compromettent pas la fonction instrumentée de sécurité, si une imprimante tombe en panne, est arrêtée, est débranchée, manque de papier ou se comporte anormalement.

Les imprimantes sont utiles pour produire des documents préliminaires relatifs aux informations de séquence d'événements (SOE), aux diagnostics et autres événements et alarmes, avec l'indication de l'heure et de la date, et l'identification par un numéro repère. Il convient que des utilitaires de formatage de comptes-rendus soient fournis.

Si la fonction d'impression comporte une mémoire tampon (les informations sont stockées, puis imprimées à la demande ou en fonction d'un scénario synchronisé), il convient alors que la mémoire tampon soit dimensionnée de sorte que les informations ne soit pas perdues, et que sous aucun prétexte, la fonctionnalité du SIS ne soit compromise du fait d'une insuffisance d'espace mémoire tampon.

a) video displays

BPCS video displays may share SIS and BPCS functions provided the displayed data is for information only. Safety critical information is additionally displayed via the SIS (for example, if the operator is part of the safety function).

When operator action is needed during emergency conditions, the update and refresh rates of the operator display should be carried out in accordance with the safety requirements specification.

Video displays relating to the SIS should be clearly identified as such, avoiding ambiguity or potential for operator confusion in an emergency situation.

The BPCS operator interface may be used to provide automatic event logging of safety instrumented functions and BPCS alarming functions.

Conditions to be logged might include the following:

– SIS events (such as trip and pre-trip occurrences);

– whenever the SIS is accessed for program changes;

– diagnostics (for example, discrepancies, etc).

It is important that the operator be alerted to the bypass of any portion of the SIS via an alarm and/or operating procedure. For example, bypassing the final element in a SIS (for example, shutoff valve) could be detected via limit switches on the bypass valve that turn on an alarm on the panel board or by installing seals or mechanical locks on the bypass valve that are managed via operating procedures. It is generally suggested to keep these bypass alarms separate from the BPCS.

b) panels

Panels should be located to give operators easy access.

Panels should be arranged to ensure that the layout of the push buttons, lamps, gauges, and other information is not confusing to the operator. Shutdown switches for different process units or equipment, which look the same and are grouped together, may result in the wrong equipment being shut down by an operator under stress in an emergency situation. The shutdown switches should be physically separated and their function labelled. Means should be provided to test all lamps.

c) printers and logging

Printers connected to the SIS should not compromise the safety instrumented function if the printer fails, is turned off, is disconnected, runs out of paper or behaves abnormally.

Printers are useful to record the sequence in which events occur, diagnostics and other events and alarms, with time and date stamping and identification by tag number. Report formatting utilities should be provided.

If printing is a buffered function (information is stored, then printed on demand or on a timed schedule), then the buffer should be sized so that information is not lost, and under no circumstances should SIS functionality be compromised due to filled buffer memory space.

11.7.1.1 Il convient que l'opérateur obtienne assez d'informations sur un affichage pour donner suite rapidement aux informations critiques. La cohérence de l'affichage est importante et il convient que les méthodes, les conventions d'alarme et les composants d'affichage utilisés soient cohérents avec ceux des afficheurs du BPCS.

La disposition d'affichage est également importante. Il convient d'éviter les dispositions présentant une grande quantité d'informations sur un afficheur, car elles peuvent conduire à de mauvaises interprétations des données de la part des opérateurs, qui pourraient entreprendre des actions incorrectes. Il convient d'utiliser des couleurs, des indicateurs clignotants et un espacement judicieux des données pour guider l'opérateur vers les informations importantes et réduire toute possibilité de confusion. Il convient que les messages soient clairs, concis et non ambigus.

Il convient que l'affichage soit conçu de telle manière que les données puissent être identifiées par l'opérateur, si ce dernier est daltonien. Par exemple, il convient que des conditions matérialisées par des couleurs rouges ou vertes soient également traduites par des graphismes pleins ou vides.

11.7.1.2 Aucune ligne directrice n'est fournie.

11.7.1.3 Aucune ligne directrice n'est fournie.

11.7.1.4 Aucune ligne directrice n'est fournie.

11.7.1.5 Aucune ligne directrice n'est fournie.

11.7.2 Exigences relatives à l'interface de maintenance/d'ingénierie

11.7.2.1 Aucune ligne directrice n'est fournie.

11.7.2.2 Les interfaces de maintenance/ingénierie consistent en des moyens de programmation, d'essais et de maintenance du SIS. Les interfaces sont des dispositifs qui sont utilisés pour des fonctions telles que

a) la configuration du matériel du système;
b) le développement du logiciel d'application, la documentation, et le téléchargement vers l'unité logique du SIS;
c) l'accès au logiciel d'application pour les modifications, les essais, et la surveillance;
d) la visualisation des ressources système du SIS et informations de diagnostic;
e) le changement des niveaux de sécurité du SIS et l'accès aux variables du logiciel d'application.

Il convient que les interfaces de maintenance/ingénierie aient les capacités d'afficher l'état de fonctionnement et de diagnostic de tous les composants du SIS (par exemple, les modules d'entrée/sortie, les processeurs), comprenant les communications entre ces derniers.

Il convient que la maintenance/ingénierie fournisse des moyens pour copier les programmes d'application sur des média de stockage, pour en assurer la sauvegarde.

Il convient qu'un ordinateur individuel connecté à un SIS pour les besoins de la maintenance/ ingénierie, ne compromette pas des fonctions de sécurité, si l'ordinateur individuel tombe en panne, est arrêté ou encore s'il est déconnecté.

11.7.2.3 Aucune ligne directrice n'est fournie.

11.7.2.4 Aucune ligne directrice n'est fournie.

11.7.1.1 The operator should be given enough information on one display to rapidly convey critical information. Display consistency is important and the methods, alarm conventions and display components used should be consistent with the BPCS displays.

Display layout is also important. Layouts with a large amount of information on one display should be avoided since they may lead to operators misreading data and taking wrong actions. Colours, flashing indicators, and judicious data spacing should be used to guide the operator to important information so as to reduce the possibility of confusion. Messages should be clear, concise and unambiguous.

The display should be designed such that data can be recognized by operators who may be colour blind. For example, conditions shown by red or green colours could also be shown by filled or unfilled graphics.

11.7.1.2 No further guidance provided.

11.7.1.3 No further guidance provided.

11.7.1.4 No further guidance provided.

11.7.1.5 No further guidance provided.

11.7.2 Maintenance/engineering interface requirements

11.7.2.1 No further guidance provided.

11.7.2.2 Maintenance/engineering interfaces consist of means to program, test and maintain the SIS. Interfaces are devices which are used for functions such as:

a) system hardware configuration;
b) application software development, documentation, and downloading to the SIS logic solver;
c) access to application software for changes, testing, and monitoring;
d) viewing SIS system resource and diagnostic information;
e) changing SIS security levels and access to application software variables.

Maintenance/engineering interfaces should be capable of displaying the operating and diagnostic status of all SIS components (for example, as input modules, processors) including the communication between them.

Maintenance/engineering should provide means for copying application programs to storage backup media.

A personal computer connected to a SIS for maintenance/engineering purposes, should not compromise safety functions if the personal computer fails, is turned off or is disconnected.

11.7.2.3 No further guidance provided.

11.7.2.4 No further guidance provided.

11.7.3 Exigences relatives à l'interface de communication

11.7.3.1 Aucune ligne directrice n'est fournie.

11.7.3.2 Aucune ligne directrice n'est fournie.

11.7.3.3 Aucune ligne directrice n'est fournie.

11.7.3.4 Aucune ligne directrice n'est fournie.

11.8 Exigences relatives à la maintenance ou à la conception des tests

11.8.1 Il convient que la conception du SIS prenne en compte la manière dont le système va être maintenu et essayé. Si le SIS doit être essayé pendant que le processus est exécuté, il convient que la conception ne nécessite pas la déconnexion de fils, l'application de connexions temporaires (cavaliers/bretelles) ou le forçage de registres du logiciel, car l'utilisation de ces techniques peut compromettre l'intégrité du SIS. Il convient que la conception du système fournisse les exigences techniques et procédurales du SIS, afin de réaliser, sans risque, les essais complets du système de capteurs, de l'unité logique et des éléments terminaux.

Il est important de définir comment un SIS va être maintenu pendant que le processus est exécuté. Par exemple, s'il est nécessaire de travailler sur un transmetteur ou sur une vanne, on doit considérer la façon dont le service de maintenance travaillera sur ces instruments, sans provoquer de déclenchement intempestif, tout en conservant la sécurité du processus.

Il convient de noter que toute limite sur la période d'essai des éléments terminaux devrait être prise en compte dans le calcul de la PFD_{avg} du SIF.

11.8.2 Aucune ligne directrice n'est fournie.

11.8.3 L'installation de dérivations peut réduire le niveau de sécurité dans un SIS. Cette réduction de sécurité peut être contournée par

a) l'utilisation de mots de passe et/ou commutateurs à verrouillage par clé. Certaines conceptions peuvent incorporer des coffrets fermant à clé (ou verrouillés) contenant les dérivations appropriées;
b) l'identification claire des dérivations de tuyauterie peut être réalisée soit par blocage des positions de vanne, soit en installant des marquages de sécurité indiquant l'importance de la position appropriée.

Par exemple, pour une configuration de capteur 1oo2, certains utilisateurs souhaitent dériver les deux capteurs en même temps, mais d'autres souhaitent avoir une dérivation séparée pour chaque capteur. Si les deux capteurs sont dérivés, il sera nécessaire de mettre en place des mesures pour s'assurer que le risque reste tolérable. L'une ou l'autre option est possible, mais il convient d'étudier les deux possibilités très tôt dans le processus de conception.

De même, certaines opérations du processus n'acceptent pas que la position de la vanne soit modifiée pendant que le processus est en cours d'exécution, ou l'installation d'une dérivation contournant la vanne peut être impraticable. Dans ces cas, il convient que la conception tienne compte des essais du SIS, autant qu'il est possible, c'est-à-dire, au moins par l'intermédiaire de l'électrovanne. Dans ce dernier cas, un certain type de dérivation autour du solénoïde peut être inclus dans la conception, avec les commandes d'alarme ou procédurales habituelles pour cette dérivation.

11.8.4 Aucune ligne directrice n'est fournie.

11.7.3 Communication interface requirements

11.7.3.1 No further guidance provided.

11.7.3.2 No further guidance provided.

11.7.3.3 No further guidance provided.

11.7.3.4 No further guidance provided.

11.8 Maintenance or testing design requirements

11.8.1 The design of the SIS should take into consideration, how the system is going to be maintained and tested. If the SIS is to be tested while the process is running, the design should not require the disconnection of wires, applying jumpers or forcing software registers since using these techniques may jeopardize the integrity of the SIS. The system design should provide technical and procedural requirements of the SIS in order to accomplish full system testing of sensors, logic solver and final elements safely.

It is important to define how a SIS is going to be maintained while the process is running. For example, if a transmitter or valve needs to be worked on, consideration needs to be given on how the maintenance department will work on these instruments without causing a nuisance trip while maintaining the safety of the process.

It should be noted that any limit on the testing period of final elements should be taken into account in the calculation of the PFD_{avg} of the SIF.

11.8.2 No further guidance provided.

11.8.3 The installation of bypasses may reduce the level of security in a SIS. This reduction in security may be overcome by:

a) Using passwords and/or key locked switches. Some designs may incorporate locked cabinets containing the appropriate bypasses.

b) Clear identification of piping bypasses may be accomplished by either sealing valve positions or installing safety signs indicating importance of the appropriate position.

For example, for a 1oo2 sensor configuration, some users like to bypass both sensors at one time but others like to have a separate bypass for each sensor. If both sensors are bypassed, it will be necessary to put measures in place to ensure that risk remains tolerable. Either can be possible, but this should be addressed early in the design.

Likewise, some process operations do not support the valve being moved while the process is running or installing a bypass around the valve may be impractical. In these cases, the design should allow for testing the SIS as far as practical, i.e., at least through the solenoid valve. In this case, some type of bypass around the solenoid can be included in the design with the usual alarming or procedural controls for this bypass.

11.8.4 No further guidance provided.

11.9 Probabilité de défaillance de la SIF

11.9.1 Les utilisateurs et les concepteurs se réfèreront à l'Annexe A de la présente norme, où ils trouveront des conseils concernant les techniques disponibles pour s'assurer que la conception du SIS satisfait aux performances relatives aux défaillances aléatoires du matériel.

11.9.2 La plupart des techniques données à l'Annexe A nécessitent une certaine quantification de la couverture du diagnostic du SIS. Les diagnostics sont des essais exécutés automatiquement pour détecter des anomalies dans le SIS, pouvant avoir comme conséquence des défaillances de sécurité ou des défaillances dangereuses.

Une technique de diagnostic particulière ne peut, habituellement, pas détecter toutes les anomalies possibles. Une évaluation de l'efficacité des dispositifs de diagnostic utilisés peut être donnée pour l'ensemble des anomalies considérées. Les paragraphes 7.4.4.5 et 7.4.4.6 de la CEI 61508-2 donnent des exigences relatives à la façon dont les diagnostics pourraient être déterminés (voir également l'Annexe C de la CEI 61508-6 pour avoir un exemple de la manière dont la couverture du diagnostic est calculée).

L'amélioration de la couverture de diagnostic du SIS peut aider à satisfaire aux exigences du SIL. Dans ce cas, il convient qu'à la fois la couverture de diagnostic et la période entre essais de diagnostic (l'intervalle des essais de diagnostic) soient prises en compte pour calculer la probabilité de la défaillance (mode de sollicitation) ou la fréquence de la défaillance (mode continu) du SIS. Pour d'autres directives il convient de se référer à la CEI 61508-6, Annexe B ou à l'ISA TR84.00.02.

Dans les situations où le SIS est la seule couche de protection, et où il est utilisé pour une fonction de sécurité fonctionnant dans le mode de fonctionnement en continu, l'intervalle des essais de diagnostic nécessitera d'être tel que les anomalies dans le SIS soient détectées à temps pour assurer l'intégrité du SIS et permettre à une action d'être entreprise pour garantir un état de sécurité dans le cas d'une défaillance se produisant dans le processus ou dans le système de commande de processus de base.

Pour réaliser ceci, il convient que la somme de l'intervalle des essais de diagnostic et du temps de réaction pour atteindre un état de sécurité soit inférieure au «temps de sécurité du processus». Le temps de sécurité du processus est défini comme étant la période de temps entre une défaillance se produisant dans le processus ou dans le système de commande de processus de base (avec la potentialité de provoquer un événement dangereux) et l'occurrence de l'événement dangereux, si la fonction instrumentée de sécurité n'est pas exécutée.

En règle générale, les anomalies critiques et potentiellement critiques des composants communs (comme des anomalies de CPU/RAM/ROM) empêchent presque totalement le traitement des données et ont donc plus d'impact qu'une anomalie d'un seul point de sortie. Les modes de défaillance qui présentent une probabilité de défaillance élevée doivent être détectés avec plus de certitude. De plus, la détectabilité des modes de défaillance doit être prise en considération.

Pour chaque dispositif de diagnostic mis en œuvre, il convient que l'intervalle des essais et l'action résultante sur la détection de l'anomalie répondent à la spécification des exigences concernant la sécurité.

Dans le cas où ces dispositifs de diagnostic ne seraient pas intégrés dans les équipements mis à disposition par le fournisseur, des dispositifs de diagnostic configurés par un organisme externe peuvent être mis en oeuvre sur le système ou au niveau de l'application afin de satisfaire au SIL pour la SIF.

11.9 SIF probability of failure

11.9.1 Users and designers should refer to Annex A of this standard for guidance in techniques available to ensure SIS design satisfies performance relating to random hardware failures.

11.9.2 Most of the techniques in Annex A of this standard require some quantification of the diagnostic coverage of the SIS. Diagnostics are tests performed automatically to detect faults in the SIS that may result in safe or dangerous failures.

A particular diagnostic technique cannot usually detect all possible faults. An estimate of the effectiveness of the diagnostics used may be provided for the set of faults being addressed. Subclauses 7.4.4.5 and 7.4.4.6 of IEC 61508-2 provide requirements for how diagnostics could be determined (see also Annex C of IEC 61508-6 for an example of how diagnostic coverage is calculated).

Improving the diagnostic coverage of the SIS may assist in satisfying the SIL requirements. In this case, both the diagnostic coverage and the period between diagnostic tests (the diagnostic test interval) should be taken into account when calculating the probability of failure (demand mode) or frequency of failure (continuous mode) of the SIS. For further guidance, refer to IEC 61508-6, Annex B or ISA TR84.00.02.

In situations where the SIS is the only layer of protection and is used for a safety function operating in the continuous mode of operation, then the diagnostic test interval will need to be such that faults in the SIS are detected in time to ensure the integrity of the SIS and to allow action to be taken to ensure a safe state in the event of a failure occurring in the process or the basic process control system.

To achieve this, the sum of the diagnostic test interval and the reaction time to achieve a safe state should be less than the “process safety time”. The process safety time is defined as the time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety instrumented function is not performed.

Critical and potentially critical faults to common components (such as faults to CPU/RAM/ROM) typically inhibit nearly the entire processing of data and are therefore more far reaching than a fault of a single output point. Failure modes that carry a high failure probability have to be detected with more confidence. Furthermore, the detectability of failure modes should be taken into account.

For each diagnostic implemented, testing interval and resulting action on fault detection should meet the safety requirements specification.

Where these diagnostics are not “built in” the vendor supplied equipment, externally configured diagnostics may be implemented at the system or application level in order to meet the SIL for the SIF.

Les dispositifs de diagnostic peuvent être incapables de détecter des erreurs systématiques (comme des erreurs de programmation). Cependant, des mesures conservatoires appropriées pour détecter des anomalies systématiques éventuelles peuvent être mises en oeuvre.

Les dispositifs de diagnostic peuvent être réalisés en utilisant diverses méthodes ou une combinaison de méthodes, incluant les éléments figurant ci-dessous.

a) Capteurs

1) Des alarmes de diagnostic peuvent être utilisées pour détecter un capteur qui délivre une indication complètement au-delà ou en deçà de la plage attendue. L'utilisation d'une alarme «hors gamme» peut être une manière de réaliser ceci. Par exemple, dans une application de déclenchement sur hautes températures, avec les transmetteurs de température redondants, une alarme «signal faible, hors gamme» pourrait être ajoutée pour diagnostiquer une défaillance de transmetteur ou une perte de signal de ce dernier.
2) Si des transmetteurs redondants sont utilisés, la comparaison des valeurs analogiques permet de détecter les anomalies qui peuvent se produire pendant l'exploitation normale. Si trois transmetteurs sont utilisés, la valeur médiane des trois lectures peut être utilisée (choix de la valeur médiane). Le choix de la valeur médiane est plus avantageux que la comparaison à la moyenne, parce que la moyenne est biaisée par le dispositif qui ne fonctionne pas correctement. Des écarts significatifs entre les lectures peuvent être créés par
   – le raccordement ou le gel au niveau des lignes de sortie d'impulsion;
   – la réduction de la pression d'alimentation de purge;
   – un revêtement relatif à un procédé de gaine thermométrique;
   – des problèmes de mise à la terre ou d'alimentation en énergie;
   – la non-réponse d'un transmetteur ayant une valeur de sortie qui reste fixe.
3) Des retards temporels peuvent être prévus pour prévenir les alarmes intempestives dues aux variations de la réponse du capteur du fait des changements de processus provoqués par l'emplacement du capteur ou par sa technologie. Par exemple, certains capteurs de débit redondants peuvent avoir une temporisation de 1 s à 2 s. Un certain nombre de progiciels proposés par des fournisseurs sont disponibles pour surveiller les lectures des capteurs redondants et calculer l'écart type, afin d'initier les alarmes de diagnostics.
4) Une autre méthode de diagnostics relative au capteur est la comparaison de variables liées (par exemple, les totalisateurs de débit en fonction d'une modification de niveau de réservoir ou relation entre pression et température).

b) Eléments terminaux

1) La comparaison des informations en retour de l'élément final (tels que des interrupteurs de fin de course ou des transmetteurs de position) par rapport à l'état requis, peut être effectuée pour vérifier que les actions prévues ont été entreprises. Il convient que des retards suffisants soient utilisés pour filtrer l'alarme relative aux vannes en cours de transition (par exemple, de complètement ouverte à complètement fermée). Cette comparaison des informations en retour de l'élément final par rapport à l'état requis ne peut être considérée comme étant un diagnostic que si la vanne change périodiquement à l'état de sécurité, dans le cadre de l'exploitation normale (par exemple, fonctionnement en lots).
2) Certaines vannes, certains actionneurs, solénoïdes, et/ou positionneurs peuvent comporter des possibilités de diagnostics.

Diagnostics may not be capable of detecting systematic errors (such as software bugs). However, appropriate precautionary measures to detect possible systematic faults may be implemented.

Diagnostics may be accomplished using a variety or combination of methods, including:

a) Sensors

1) Diagnostic alarms could be provided to detect a sensor that has completely failed upscale or downscale. One way this can be accomplished is by use of an out of range alarm. For example, in a high temperature trip application with redundant temperature transmitters, a low out of range alarm could be added to diagnose a transmitter failure or loss of transmitter signal.

2) If redundant transmitters are used, comparison of the analogue values detects anomalies that may occur during normal operation. If three transmitters are used, the middle of the three readings can be used (mid-value selection). Mid value selection is advantageous over comparison to the average because the average is skewed by the device that is not functioning properly. Significant deviations between readings may be created by

   − plugging or freezing in the impulse leads;

   − reduction in purge supply pressure;

   − process coating of thermowells;

   − grounding or power supply problems;

   − non-response of a transmitter that has an output value that is no longer changing.

3) Time delays may be provided to prevent nuisance alarms due to variations in sensor response to process changes caused by sensor location or sensor technology. For example, some redundant flow sensors may have 1 to 2 s delays. There are a number of software packages available from vendors to monitor redundant sensor readings and calculate the standard deviation in order to initiate the diagnostic alarms.

4) Another method of sensor diagnostics is comparison of related variables (for example, flow totalizers versus tank level changes or pressure and temperature relationship).

b) Final elements

1) Comparison of the feedback from the final element (such as limit switches or position transmitters) to the requested state may be performed to verify that the expected actions have been taken. Sufficient time delays should be used to filter the alarm for valves in transition (for example, from fully opened to fully closed). This comparison of the feedback from the final element to the requested state can only be considered to be a diagnostic if the valve periodically changes to the safe state as part of normal operation (for example, batching operation).

2) Some valves, actuators, solenoids, and/or positioners may provide diagnostic capability.

c) Unités logiques

Les unités logiques à électronique programmable (PE) qui sont configurées pour la sécurité ou conformes à la CEI 61508 incluent généralement des dispositifs de diagnostic, détectant différentes anomalies. Les types et la couverture de diagnostic sont généralement décrits dans le manuel de sécurité.

d) Dispositifs de diagnostic configurés extérieurement

Les exemples de ces derniers comprennent les horloges de surveillance et les dispositifs de surveillance d'extrémité de ligne.

Concernant la note du point c) de 11.9.2 relative au niveau de confiance par rapport aux données de fiabilité, le temps moyen entre défaillances (MTTF) est typiquement déterminé en enregistrant le nombre de défaillances (n) qui se produisent dans un échantillon de composants pendant un nombre d'heures d'exploitation cumulée (t). Un niveau de confiance dans le MTTF résultant peut être dérivé en utilisant l'essai du Khi-deux (khi^2) (se référer à *Fiabilité, maintenabilité et risque*, D J Smith ISBN 0 7506 5168 7). Ceci signifie que la valeur de MTTF à utiliser dans les calculs de fiabilité, pour un SIS, sera, en général, inférieure à la valeur du MTTF calculé comme *T*/*n*. Ce facteur de réduction sera plus grand pour un niveau de confiance requis plus élevé et pour un nombre de défaillances observées plus faible. Cependant, en général, il est raisonnable de supposer qu'à un niveau de confiance de 70 %, le facteur de réduction n'est pas significatif comparé à d'autres sources d'incertitude, associées à la modélisation de la fiabilité.

12 Exigences relatives au logiciel d'application, incluant les critères de sélection pour le logiciel utilitaire

L'Article 12 de la CEI 61511-1 ne fait pas la différence entre les méthodes de conception du logiciel d'application de SIL 3 et de SIL inférieurs, parce que l'expérience montre qu'il y a peu de différence entre les méthodes, en utilisant:

– soit les FPL, soit les LVL; et
– une unité logique conforme à la CEI 61511; et
– le manuel de sécurité correspondant.

Il peut y avoir des différences en ce qui concerne les essais et la vérification pour différents SIL. Voir 12.7.2.3 pour d'autres directives.

12.1 Exigences relatives au cycle de vie de sécurité du logiciel d'application

12.1.1 Objectifs

12.1.1.1 Aucune ligne directrice n'est fournie.

12.1.2 Exigences

12.1.2.1 Aucune ligne directrice n'est fournie.

12.1.2.2 Notes 1 et 2: Lorsque des langages de variabilité limitée, tels que le langage à contacts de la CEI 61131-3 ou le langage en blocs fonctionnels, sont utilisés pour la conception, la mise en oeuvre, la vérification et la validation du logiciel d'application, il n'est alors nécessaire d'appliquer que deux niveaux du modèle standard de logiciel en «V» représenté par la Figure 3. Dans ce cas, il est supposé que les blocs fonctionnels utilisés satisfont à la CEI 61508-3, alors:

– la «conception de l'architecture du logiciel d'application» est appliquée au logiciel pour chaque SIF, d'une manière qui garantit que la conception du logiciel est cohérente avec l'architecture du matériel;

c) Logic Solvers

Safety-configured or IEC 61508 series compliant PE logic solvers typically include diagnostics which detect various faults. The types and diagnostic coverage will generally be described in the Safety Manual.

d) Externally configured diagnostics

Examples of these include watchdog timers and end-of-line monitors.

With reference to the Note in 11.9.2.c) of IEC 61511-1 regarding confidence in reliability data, mean time to failure (MTTF) is typically determined by recording the number of failures (n) which occur in a sample of components during an accumulated number of operating hours (T). A confidence level in the resulting MTTF can be derived using the 'Chi-square' test (see '*Reliability, maintainability and risk*, D J Smith' ISBN 0 7506 5168 7). This means that the value of MTTF to be used in the reliability calculations for a SIS will, in general, be lower than the value of MTTF calculated as T/n. This reduction factor will be greater for a higher required confidence level and for lower numbers of observed failures. However, in general, it is reasonable to assume that at a 70 % confidence level the reduction factor is not significant compared to other sources of uncertainty associated with reliability modelling.

12 Requirements for application software, including selection criteria for utility software

Clause 12 of IEC 61511-1 does not differentiate between SIL 3 and lower SIL application software design methods because experience shows that there is little difference in the methods when using:

- either FPLs or LVLs; and
- IEC 61511-1 compliant logic solver; and
- the corresponding Safety Manual.

There may be differences for test and verification for different SILs. See 12.7.2.3 of this part for guidance.

12.1 Application software safety lifecycle requirements

12.1.1 Objective

12.1.1.1 No further guidance provided.

12.1.2 Requirements

12.1.2.1 No further guidance provided.

12.1.2.2 Notes 1 and 2: When limited variability languages such as IEC 61131-3 ladder diagram or function block diagram are used for the design, implementation, verification and validation of application software, then only two levels of the standard software "V" model shown in Figure 3 need apply. In this case, it is assumed that the used function blocks conform to IEC 61508-3, then:

- "application software architecture design" is applied to the software for each SIF in a way that ensures the software design is consistent with the hardware architecture;

– le «développement du logiciel d'application» est interprété comme la conception et la mise en œuvre de la logique de sécurité, utilisant le langage de variabilité limitée conforme à la CEI 61508;

– les «essais du logiciel d'application» sont interprétés comme la vérification et l'essai du logiciel d'application; et

– «l'intégration du logiciel d'application avec le sous-système du SIS» est interprété comme l'intégration et la vérification de chaque fonction de sécurité du processus mis en oeuvre dans le langage de variabilité limitée.

Un exemple d'un cycle de vie de développement de logiciel d'application, utilisant un PLC conforme à la CEI 61508, SIL 3, est donné en Annexe D.

Lorsqu'une nouvelle «fonction» ou un nouveau «bloc fonctionnel» est à mettre en œuvre en utilisant des éléments du langage de variabilité limitée conforme à la CEI 61508 (par exemple, mise en oeuvre d'une séquence de verrouillage de brûleur commun ou d'une séquence de verrouillage de pompe) alors:

– le «développement du module d'application» dans le modèle en «V» est interprété comme la conception et la mise en oeuvre de la nouvelle fonction; et

– les «essais du module d'application» sont interprétés comme la vérification et les essais de la nouvelle fonction.

Dans le cas où une nouvelle fonction serait à écrire dans un langage de variabilité totale et donc où le développement du code logiciel serait nécessaire, il conviendrait que le développeur suive toutes les phases et procédures du cycle de vie définies par la CEI 61508-3alors, comme le modèle en «V» (Figure 3) l'indique.

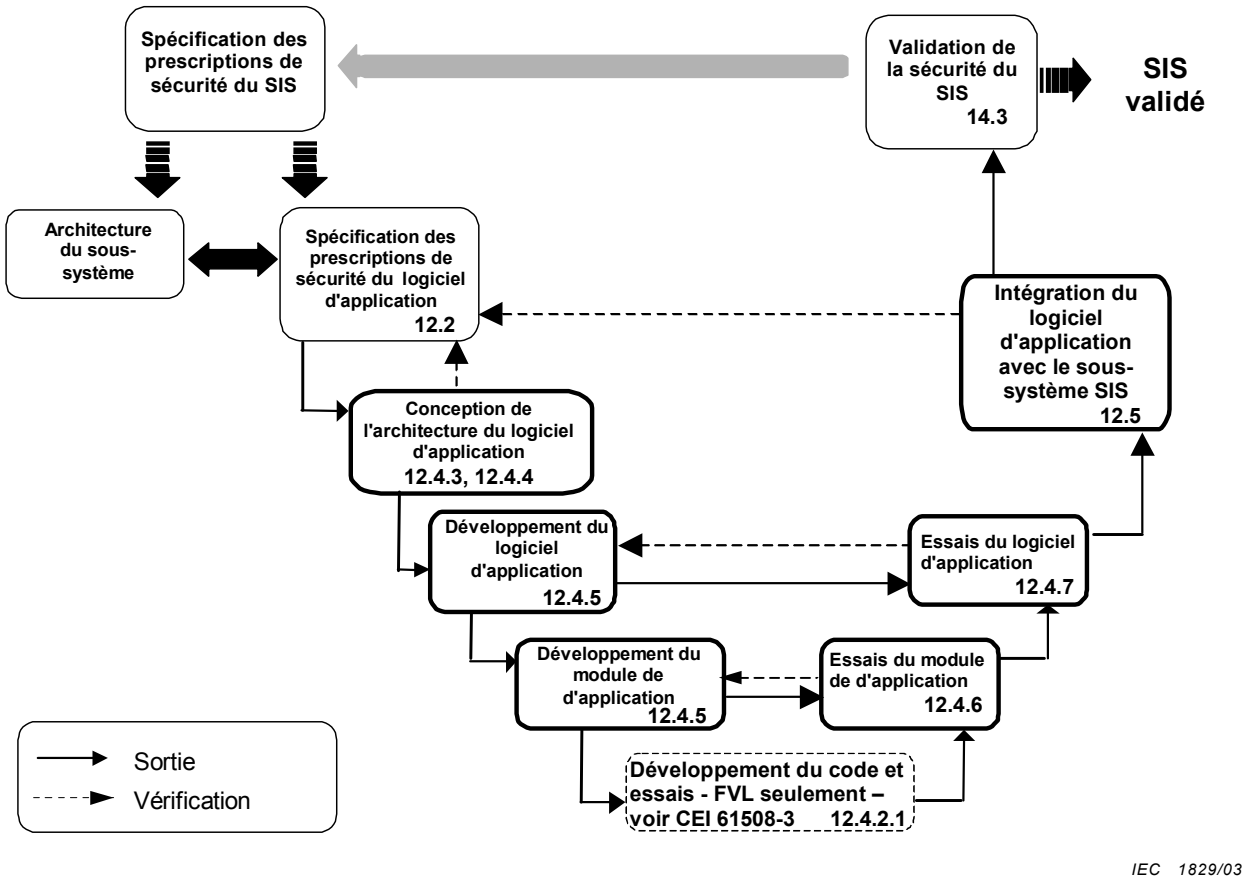


Figure 3 – Cycle de vie de développement du logiciel d'application(modèle en V)

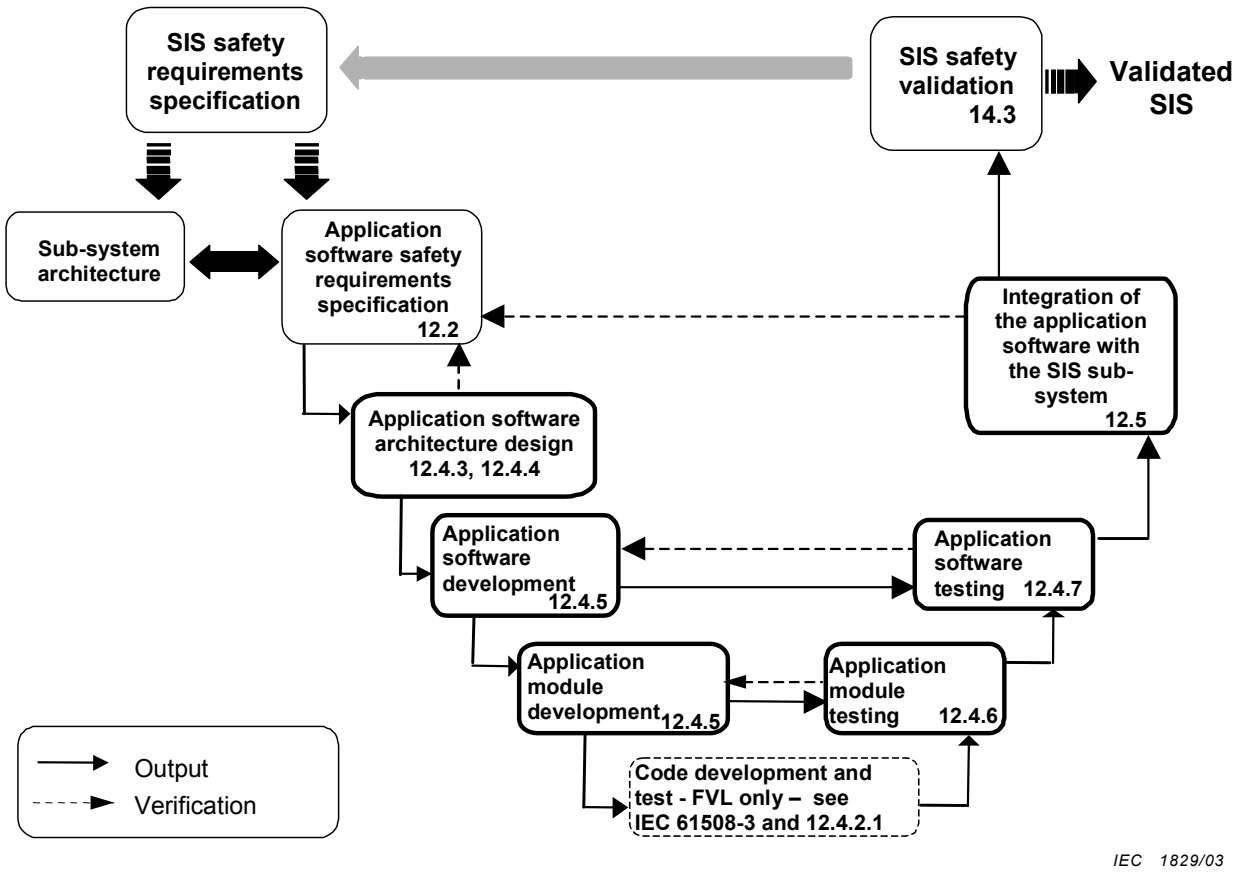
- ”application software development” is interpreted as the design and implementation of the safety logic using the IEC 61508-3 and IEC 61508-4 compliant limited variability language;
- “application software testing” is interpreted as the verification and test of the application software; and
- “Integration of the application software with the SIS subsystem” is interpreted as the integration and verification of each process safety function implemented in the limited variability language.

An example of an application software development lifecycle using an IEC 61508 series SIL 3 compliant PLC is given in Annex D.

Where a new “function” or “function block” is to be implemented using elements of the IEC 61508 series compliant Limited Variability Language (for example, implementation of a common burner interlock sequence or pump interlock sequence) then:

- “Application Module Development” in the “V” model is interpreted as the design and implementation of the new function; and
- “Application Module Testing” is interpreted as the verification and testing of the new function.

In the case where a new function is to be written in a full variability language and therefore software code development is needed, then, as the “V” model (Figure 3) indicates, the developer should follow all of the lifecycle phases and procedures defined in IEC 61508-3.



NOTE Unless otherwise indicated, subclause numbers in this figure refer to IEC 61511-1.

Figure 3 – Software development lifecycle (the V-model)

12.1.2.3 Aucune ligne directrice n'est fournie.

12.1.2.4 Des considérations relatives au choix de méthodes, de techniques et d'outils sont données ci-après:

Pour choisir les méthodes, les techniques et les outils qui peuvent contribuer au fait que le logiciel aura la qualité exigée, il faut considérer les paramètres de qualité clés suivants concernant le logiciel d'application:

– la simplicité;
– l'aide de commentaires appropriés et en langage naturel;
– la compartimentation pour refléter l'application;
– la couverture des essais;
– la compréhension par le personnel impliqué dans le processus d'aide;
– les similitudes avec d'autres logiciels d'application proches.

Les approches pour identifier les paramètres importants comprennent:

– les discussions avec les parties intéressées, y compris l'exploitation et la maintenance;
– la revue des pratiques en vigueur et des normes de l'industrie;
– la revue des recommandations du constructeur;
– l'analyse des expériences précédentes;
– les discussions avec des confrères.

Il convient de choisir les méthodes, les techniques et les outils pour optimiser les paramètres de qualité importants en tenant compte des considérations ci-dessous.

Il convient que les méthodes et les techniques soient choisies de manière à minimiser le risque de présenter des anomalies dans le logiciel d'application pendant le développement. On peut alors considérer

– une syntaxe et une sémantique bien définies;
– l'adéquation à l'application;
– la compréhension par les développeurs de l'application;
– la garantie des propriétés importantes pour la SIF (par exemple, le pire cas des temps d'exécution);
– les preuves/justifications d'une utilisation satisfaisante dans des applications similaires;
– les règles et les contraintes visant à limiter l'utilisation des dispositions «dangereuses» de la méthode.

Il convient que les outils soient choisis pour mettre en oeuvre des méthodes et des techniques destinées à réduire l'erreur humaine dans leur application pratique. On peut alors prendre en considération

– la connaissance des outils par les membres concernés de l'équipe de développement;
– les preuves/justifications d'une utilisation satisfaisante des outils dans des applications similaires;
– les règles et les contraintes visant à limiter l'utilisation des fonctionnalités «dangereuses» des outils.
– la liste documentée de la version précise de tous les outils et du SIS;
– la compatibilité entre les différents outils et avec le SIS;
– la capacité à produire la documentation du logiciel d'application.

12.1.2.3 No further guidance provided.

12.1.2.4 The following are considerations for the selection of methods, techniques and tools:

To select methods, techniques and tools that may contribute towards the software having the required quality, consider the following key quality parameters for the application software:

- simplicity;
- suitable commentary and natural language support;
- compartmentalization to reflect the application;
- test coverage;
- understandability by personnel involved in the support process;
- commonality of style with other related application software.

Approaches to identifying the important parameters include

- discussions with stakeholders including operations and maintenance;
- review of current practice and industry standards;
- review of manufacturer's recommendations;
- analysis of previous experience;
- discussions with peers.

Select the methods, techniques and tools to optimise the important quality parameters taking into account the considerations below.

Methods and techniques should be selected to minimize the risk of introducing faults into the application software during development. This may include the consideration of

- well-defined syntax and semantics;
- suitability for the application;
- understandability by the application developers;
- guarantee of properties important to the SIF (for example, worst case execution time);
- evidence of successful use in similar applications;
- rules and constraints aimed at restricting the use of "unsafe" features of the method.

Tools should be selected to implement the methods and techniques so as to reduce human error in their practical application. This may include the consideration of

- familiarity with tools by the appropriate members of the development team;
- evidence of successful use of the tools in similar applications;
- rules and constraints aimed at restricting the use of "unsafe" features of the tools;
- documented list of the precise version of all tools and the SIS;
- compatibility between the different tools and with the SIS;
- ability to generate application software documentation.

Des exemples typiques d'outils utilisés pendant les phases du cycle de vie comprennent

– des générateurs de code d'application;
– la gestion de configuration;
– des analyseurs statiques (par exemple, contrôleur de nom d'étiquette, contrôleur de temps de balayage);
– des simulateurs;
– des bancs d'essai comprenant des programmes d'essai de logiciels;
– une station de travail d'ingénierie.

D'autres méthodes, techniques et outils qui pourraient être considérés, comprennent des mesurages (par exemple, couverture d'essai) et l'utilisation de différents outils pour améliorer la vérification d'une ou de plusieurs fonctions (par exemple, outils dos à dos).

Afin de révéler et d'éliminer les anomalies qui existent déjà dans le logiciel, une vérification est recommandée tout au long du cycle de vie du développement. Des approches typiques sont décrites en 12.7.2.3.

Pour s'assurer que les anomalies restantes dans le logiciel ne conduiront pas à des résultats inacceptables, les points suivants peuvent être considérés:

– les techniques de vérification et traitement d'exception «en ligne»;
– l'utilisation de bases de données commerciales externes et de comptes-rendus d'anomalies globaux;
– la surveillance des comptes-rendus de défaillance du SIS et des problèmes de processus et de leur impact sur le SIS;
– la redondance des fonctionnalités importantes du SIS par enregistrement dans d'autres systèmes;
– l'utilisation d'une copie du logiciel d'application du SIS pendant le cursus de formation.

Pour s'assurer que le logiciel peut être maintenu pendant toute la vie du SIS, les points suivants peuvent être considérés:

– le programme pour la gestion des modifications (voir la CEI 61511-1, Article 17);
– l'aide permanente à la gestion et la formation à la maintenance;
– la disponibilité des outils d'aide et de la plate-forme de développement pendant toute la vie du SIS;
– des méthodes bien documentées et de préférence largement utilisées, pour faciliter les ressources humaines et les qualifications adaptées pendant toute la vie du SIS;
– l'utilisation de règles de développement et de documentation visant à faciliter la compréhension et à limiter les effets des modifications du logiciel;
– la documentation «conforme à l'exécution» et à jour;
– l'aptitude à développer et à essayer «hors-ligne».

12.1.2.5 Aucune ligne directrice n'est fournie.

12.1.2.6 Aucune ligne directrice n'est fournie.

12.1.2.7 Aucune ligne directrice n'est fournie.

12.1.2.8 Aucune ligne directrice n'est fournie.

Typical examples of tools used during the lifecycle phases include:

- application code generators;
- configuration management;
- static analysers (for example, tag name checker, scan time checker);
- simulators;
- test harnesses including software test programs;
- engineering workstation.

Other methods, techniques and tools that could be considered include metrics measurements (for example, test coverage) and use of different tools to enhance verification of a function(s) (for example, back-to-back tools).

In order to reveal and remove faults that already exist in the software, verification is recommended throughout the development lifecycle. Typical approaches are described in 12.7.2.3.

To ensure that the faults remaining in the software will not lead to unacceptable results, the following could be considered:

- on-line checking techniques and exception handling;
- use of vendor offsite databases and global fault reporting;
- monitoring of SIS failure reports and of process issues and their impact on the SIS;
- mirroring of key SIS functionality in other systems;
- use of a duplicate of the SIS application software during the training process.

To ensure that the software can be maintained throughout the lifetime of the SIS, the following could be considered:

- program for management of change (see Clause 17 of IEC 61511-1);
- ongoing management support and maintenance training;
- availability of support tools and development platform throughout the lifetime of the SIS;
- well-documented and preferably widely used methods to facilitate adequate human resources and skills throughout the life of the SIS;
- use of development and documentation rules aiming at facilitating understanding and limiting the effects of changes in software;
- ‘as-built’ and up-to-date documentation;
- ability to develop and test off-line.

12.1.2.5 No further guidance provided.

12.1.2.6 No further guidance provided.

12.1.2.7 No further guidance provided.

12.1.2.8 No further guidance provided.

12.2 Spécification des exigences de sécurité du logiciel d'application

12.2.1 Objectif

12.2.1.1 Aucune ligne directrice n'est fournie.

12.2.2 Exigences

L'architecture globale du SIS peut imposer des exigences logicielles fonctionnelles supplémentaires aux fonctions instrumentées de sécurité spécifiées. Un exemple typique est la logique de sélection 1oo2 pour les capteurs redondants, ainsi qu'une action de sécurité spécifiée à la détection d'une défaillance dangereuse par auto-diagnostics au niveau du capteur. Les exemples donnés en Annexe B énumèrent ces exigences, découlant de l'architecture appliquée.

Il convient que le logiciel d'application prenne également en considération les diagnostics fournis par le PES et soit développé pour entreprendre les actions appropriées définies par le manuel de sécurité de l'unité logique.

Les exigences détaillées de sécurité pour chaque fonction instrumentée de sécurité peuvent habituellement être définies au moyen des diagrammes logiques ou des schémas «de cause à effet». Dans de nombreux cas, les langages de programmation livrés par le fournisseur de l'unité logique peuvent être utilisés pour définir les exigences. Les langages habituels qui peuvent être utilisées sont les langages en blocs fonctionnels ou à matrice de cause à effet. Il convient que le langage choisi livré par le fournisseur satisfasse à l'application. L'utilisation des langages livrés par le fournisseur pour définir les exigences détaillées peut souvent éviter les erreurs qui se produisent dans la traduction des exigences à partir d'autres formes de documentation. Il convient qu'une large l'utilisation des commentaires soit faite pour définir les fonctions de sécurité et de non-sécurité et les exigences du SIL de toutes les fonctions de sécurité.

Il convient que la spécification relative aux exigences fonctionnelles détaillées concernant la sécurité inclue toutes les fonctions nécessaires durant tous les modes de fonctionnement du processus protégé. En plus, il convient que les essais périodiques de toutes les fonctions instrumentées de sécurité soient fournis. Cela exige habituellement la définition des possibilités de maintenance prioritaire, ainsi les capteurs et les éléments terminaux peuvent être essayés sans arrêter le processus. La même méthodologie que celle décrite à l'alinéa ci-dessus peut être utilisée pour documenter ces exigences.

Si plusieurs SIS sont utilisés pour mettre en oeuvre des fonctions instrumentées de sécurité, il convient que la documentation soit fournie pour expliquer quelles fonctions sont à mettre en application dans chaque SIS. Si plusieurs SIS sont utilisés pour mettre en oeuvre la même fonction instrumentée de sécurité, il convient alors que l'interaction et l'indépendance de chaque SIS soient documentées. Il convient que cette documentation comprenne le SIL attendu, qui devrait être fourni par chaque SIS.

Pour obtenir des directives supplémentaires, il convient de se référer aux Paragraphes 10.2.1 et 10.3.1.

12.2.2.1 Aucune ligne directrice n'est fournie.

12.2.2.2 Avant le développement du logiciel d'application, l'utilisateur fournit une analyse de danger et de risque du processus, qui est utilisée pour identifier les exigences concernant la sécurité du logiciel en termes de fonctions instrumentées de sécurité et de leur SIL. Une fois que la décision pour mettre en oeuvre les fonctions instrumentées de sécurité dans le logiciel a été prise, il convient que tous les conflits, toutes les divergences et omissions dans la spécification des exigences concernant la sécurité, qui viennent à la connaissance des concepteurs du logiciel, soient traités. Un exemple pourrait être l'effet de l'ordre d'exécution de fonctions instrumentées de sécurité au sein du logiciel. Un autre exemple serait la réponse du logiciel d'application en fonction des pannes d'alimentation.

12.2 Application software safety requirements specification

12.2.1 Objective

12.2.1.1 No further guidance provided.

12.2.2 Requirements

The overall SIS architecture may impose additional functional software requirements to the specified safety instrumented functions. A typical example is the 1oo2 selection logic for redundant sensors as well as a specified safe action on detection of a dangerous failure by sensor self-diagnostics. Examples given in Annex B list those requirements originated from the applied architecture.

The application software should also take into consideration the diagnostics provided by the PES and be developed to take the appropriate actions defined in the logic solver Safety Manual.

The detailed safety requirements for each safety instrumented function can typically be defined by use of logic diagrams or cause and effect drawings. In many cases, the programming languages provided by the logic solver vendor can be used to define the requirements. Typical languages that can be used are function block diagram or cause effect matrix. The vendor supplied language selected should be suitable for the application. The use of the vendor supplied languages to define the detailed requirements can often avoid errors that occur in the translation of the requirements from other forms of documentation. Liberal use of comments should be provided to define safety and non-safety functions and the SIL requirements of all safety functions.

The detailed functional safety requirements specification should include all necessary functions during all modes of operation of the process being protected. Additionally, the periodic testing of all the safety instrumented functions should be provided. This typically requires the definition of maintenance override capabilities so the sensors and final elements can be tested without shutting down the process. The same methodology described in the paragraph above can be used to document these requirements.

If multiple SIS are used to implement safety instrumented functions, documentation should be provided to explain which functions are to be implemented in each SIS. If multiple SIS are used to implement the same safety instrumented function then the interaction and independence of each SIS should be documented. This documentation should include the expected SIL that should be provided by each SIS.

For additional guidance, refer to 10.2.1 and 10.3.1 of this standard.

12.2.2.1 No further guidance provided.

12.2.2.2 Prior to development of the application software, the user provides a process risk and hazard assessment which is used to identify the software safety requirements in terms of the safety instrumented functions and their SIL. Once the decision to implement the safety instrumented functions in software is made, any conflicts, discrepancies and omissions in the safety requirements specification which come to the attention of the software designers should be addressed. One example might be the effect of the order of execution of the safety instrumented functions within the software. Another example would be the response of the application software as it relates to energy outages.

12.2.2.3 Il convient que les exigences concernant la sécurité du logiciel d'application soient développées en tant que réponse traçable par rapport à la spécification des exigences concernant la sécurité de la SIF. Les points à traiter comprennent

– les exigences de fonctionnalité et de relations temporelles qui sont nécessaires pour mettre en oeuvre la SIF définie par l'utilisateur;
– l'interface du système logiciel avec le processus et le personnel;
– les relations entre les dangers du processus et la fonctionnalité fournie par le logiciel d'application;
– les limites du comportement du logiciel d'application qui sont autorisées, afin de rester dans l'enveloppe de sécurité du processus (par exemple, incapacité à traiter des conditions d'entrée incorrectes);
– la fonctionnalité admissible du logiciel utilitaire fourni au sein de l'unité logique, (par exemple, hiérarchisation de la logique de sécurité et des E/S par rapport aux communications, traitement d'erreur et diagnostics du système);
– la plate-forme du matériel et le logiciel système sur lequel le logiciel d'application s'exécute et la configuration du matériel et du logiciel système;
– les dangers qui pourraient survenir dans le processus, en raison de la fonctionnalité du système dont le logiciel fait partie (par exemple, modes de défaillance du matériel inadéquats lors d'une coupure d'alimentation);
– les contraintes sur les méthodes et les procédures qui pourraient être utilisées par les concepteurs, découlant du manuel de sécurité pour l'unité logique de soutien.

Afin d'éviter des difficultés lors des étapes ultérieures du processus de développement, il est également important de considérer la stratégie par laquelle il est prévu de montrer que les exigences du logiciel d'application ont été remplies.

Dans le cas où le logiciel d'application serait utilisé dans le système instrumenté de sécurité, l'évaluation fonctionnelle de sécurité pourrait comprendre:

– des techniques d'inspection pour montrer que les fonctions du logiciel d'application remplissent les exigences de danger du processus;
– des essais fonctionnels pour montrer que le logiciel d'application a exécuté les fonctions requises et, autant que possible, que toute fonctionnalité supplémentaire dans le logiciel ne risque pas d'avoir comme conséquence des conditions dangereuses;
– des essais structuraux pour montrer que le logiciel d'application a exécuté les fonctions requises dans les temps nécessaires;
– une analyse de défaillance fonctionnelle et une analyse «et si» pour montrer que les fonctions du logiciel d'application ne risquent pas d'avoir comme conséquence des conditions dangereuses;
– un audit pour montrer qu'un processus maîtrisé de développement et de vérification est en place et que la version correcte du logiciel est en service.

12.2.2.4 Aucune ligne directrice n'est fournie.

12.2.2.5 Aucune ligne directrice n'est fournie.

12.2.2.6 Aucune ligne directrice n'est fournie.

12.2.2.3 The application software safety requirements should be developed as a traceable response to the SIF safety requirements specification. Factors to be addressed include:

- functionality and timing requirements needed to implement the user-defined SIF;
- software system's interface with the process and people;
- relationship between the process hazards and the functionality provided by the application software;
- boundaries of behaviour of the application software which are permitted in order to remain within the safety envelope of the process (for example, inability to deal with erroneous input conditions);
- allowable functionality of the utility software provided within the logic solver, (for example, prioritisation of the safety logic and I/O over communications, error handling and system diagnostics;
- hardware platform and system software on which the application software executes and the configuration of the hardware and system software;
- hazards which could arise in the process as a result of the functionality of the system of which the software is a part (for example, inappropriate hardware failure modes on removal of power);
- constraints on the methods and procedures which could be used by the designers as a result of the Safety Manual for the supporting logic solver.

In order to avoid difficulties at later stages of the development process, it is also important to consider the strategy by which it was intended to show that the application software requirements had been achieved.

Where application software is used in the safety instrumented system, the functional safety assessment may include:

- inspection techniques to show that the application software functions achieve the process hazard requirements;
- functional testing to show that the application software executed the required functions and, as far as possible, that any extra functionality in the software would not result in hazardous conditions;
- structural testing to show that the application software executed the required functions in the necessary timing;
- functional failure analysis and "what if" analysis to show that application software functions would not result in hazardous conditions;
- audit to show that a controlled process of development and verification is in place and the correct software version is in use.

12.2.2.4 No further guidance provided.

12.2.2.5 No further guidance provided.

12.2.2.6 No further guidance provided.

12.3 Planification de la validation de la sécurité du logiciel d'application

Pour obtenir des directives supplémentaires, voir 14.3.

12.3.1 Objectif

12.3.2 Exigences

12.3.2.1 Aucune ligne directrice n'est fournie.

12.4 Conception et développement du logiciel d'application

12.4.1 Objectifs

12.4.1.1 Aucune ligne directrice n'est fournie.

12.4.1.2 Aucune ligne directrice n'est fournie.

12.4.1.3 Aucune ligne directrice n'est fournie.

12.4.1.4 Aucune ligne directrice n'est fournie.

12.4.1.5 Aucune ligne directrice n'est fournie.

12.4.2 Exigences générales

Un certain nombre d'approches sont possibles pour obtenir un logiciel d'application sûr dans les SIS. Cependant, indépendamment de l'approche utilisée pour réaliser un logiciel d'application sûr, il est supposé que les étapes du cycle de vie de sécurité, préalablement au développement du logiciel d'application, ont été exécutées correctement (par exemple, analyse de danger et de risque, développement de la description fonctionnelle, choix des équipements [matériel et logiciel]).

Lorsque l'installation ne peut pas s'appuyer sur une expérience préalable dans le domaine, et ne dispose d'aucune possibilité d'aide ou de dépannage, une formation assortie d'une expérience pratique (de préférence dans une application non sécuritaire) est recommandée avant la mise en oeuvre de l'approche suivante. Pour intensifier cet effort, il convient qu'une liaison avec d'autres utilisateurs d'unité logique à électronique programmable (PE), des mêmes équipements, dans le même environnement soit établie. Le degré de confiance en cette approche est un facteur important pour la détermination de l'application de l'unité logique à électronique programmable (PE), dans l'application du SIS.

Une liste de points à considérer lors du développement du logiciel d'application pour les SIS est donnée ci-après:

– scinder le logiciel d'application en SIF discrètes, avec un SIL pour chaque SIF;
– comprendre l'architecture matérielle de chaque SIF et reproduire ce matériel dans chaque logiciel d'application de la SIF;
– ne pas optimiser le logiciel d'application si cela conduit à une complexité excessive (ceci nécessite souvent un programmeur de haut niveau pour interpréter le logiciel d'application);
– utiliser les techniques de développement du logiciel d'application issues des instructions du fournisseur (par exemple, manuel de sécurité);
– ne pas combiner le logiciel d'application d'une SIF avec toute autre SIF;
– utiliser le langage du logiciel d'application (par exemple, type, fonction) pour lequel le personnel de l'installation a été formé, est capable de le comprendre et de le dépanner;

12.3 Application software safety validation planning

For additional guidance, see 14.3.

12.3.1 Objective

12.3.2 Requirements

12.3.2.1 No further guidance provided.

12.4 Application software design and development

12.4.1 Objectives

12.4.1.1 No further guidance provided.

12.4.1.2 No further guidance provided.

12.4.1.3 No further guidance provided.

12.4.1.4 No further guidance provided.

12.4.1.5 No further guidance provided.

12.4.2 General requirements

There are a number of approaches to providing safe application software in SISs. However, regardless of the approach used to achieve safe application software, it is assumed that the safety life cycle steps prior to application software development have been executed properly (for example, hazard and risk assessment, functional description development, equipment (hardware and software) selection).

When the facility has no experience, support, or troubleshooting capability, then prior to implementing the following approach, training and operating experience (preferably in a non safety application) is recommended. To enhance this effort, a liaison with other PE logic solver users of the same equipment in the same environment should be established. The degree of confidence in this approach is a major factor in determining the application of the PE logic solver in the SIS application.

Following is a list of items to consider when developing application software for SISs.

- break the application software into discrete SIF with a SIL for each SIF;
- understand the hardware architecture of each SIF and duplicate this hardware in each SIF application software;
- do not optimise the application software if this leads to excessive complexity (this often requires an advanced programmer to interpret the application software);
- use application software development techniques from the vendor instructions (for example, Safety Manual);
- do not combine application software from one SIF with any other SIF;
- use application software language (for example, type, function) in which the facility is trained, capable of understanding and troubleshooting;

– fournir la description écrite du logiciel d'application, cohérente avec la description fonctionnelle, regroupée avec la documentation du logiciel d'application;

– mettre le logiciel d'application sous forme de modules, de façon cohérente avec le déroulement du processus (par exemple, le 1er module est le logiciel d'application commun, non relatif à une SIF, mais requis dans le SIS, le 2ème module est la 1ère SIF située à l'entrée du processus, le dernier module est la dernière SIF située à la sortie du processus);

– essayer complètement (par exemple, simuler, inspecter, passer en revue) chaque module du logiciel d'application et obtenir la 2ème analyse indépendante (inclure ici le service opérationnel et de maintenance et dans toutes les étapes suivantes); essayer complètement la combinaison des modules qui composent un sous-système du processus et obtenir la 2ème analyse indépendante;

– essayer complètement le logiciel d'application du SIS;

– obtenir la 2ème analyse indépendante;

– utiliser le logiciel d'application en vérifiant le matériel (par exemple, en confirmant que les E/S sont connectées au capteur correct/à l'élément terminal correct);

– inclure les essais du logiciel d'application dans les essais «blanc» du processus (par exemple, fonctionnement du processus sans matériel dangereux);

– les membres de l'équipe de l'assistance au logiciel d'application doivent être disponibles sur l'installation pendant le déroulement du processus (par exemple, à la mise en service).

La documentation du logiciel d'application sera utilisée pour déterminer l'adéquation de ce dernier à chaque SIL de SIF. Il convient de faire une analyse indépendante pour déterminer si le logiciel d'application satisfait au SIL.

La CEI 61508-3 et la CEI 61508-6 donnent des approches alternatives et d'autres directives en cette matière.

12.4.2.1 Aucune ligne directrice n'est fournie.

12.4.2.2 En ce qui concerne les directives sur le choix des méthodes et des techniques de conception du logiciel d'application, il convient que les systèmes répondant à une exigence de sécurité de SIL 3 ou inférieure, soient conçus selon les instructions données par le manuel de sécurité des fournisseurs, en tant qu'élément d'un système conforme à la CEI 61508. Pour des systèmes de SIL 4, il convient que le développeur confirme que, de plus, les méthodes choisies sont bien conformes aux exigences de la Partie 3 de la CEI 61508.

En ce qui concerne les directives sur le choix des méthodes et des techniques d'essai et de vérification du logiciel d'application, il convient que les systèmes avec une prescription de sécurité de SIL 3 ou inférieure soient vérifiés selon les directives données en 12.7. Pour des systèmes de SIL 4, il convient que l'opérateur chargé de la vérification confirme également que les méthodes choisies sont bien conformes aux exigences de la Partie 3 de la CEI 61508.

12.4.2.3 Aucune ligne directrice n'est fournie.

12.4.2.4 En général, afin d'assurer l'aptitude aux essais, il est recommandé que les spécifications d'essai d'intégration du logiciel d'application soient examinées pendant la phase de conception et de développement.

12.4.2.5 Dans le cas où le logiciel d'application dans un SIS devrait mettre en oeuvre des fonctions instrumentées de sécurité avec des SIL différents, il conviendrait qu'elles soient clairement séparées et identifiées. Ceci permet au logiciel de chaque fonction instrumentée de sécurité de pouvoir remonter au capteur adéquat et à la redondance de l'élément terminal. Il permet également aux essais fonctionnels et de validation des fonctions d'être proportionnés au SIL. Il convient que des marquages identifient le SIF et le SIL.

- provide a written description of the application software consistent with the functional description, located with the application software documentation;
- modularise the application software consistent with the process flow (for example, the first module is common application software which is not SIF related but which is required in the SIS, the second module is the first SIF located at the process inlet, the last module is the last SIF located at the process outlet);
- thoroughly test (for example, simulate, inspect, review) each application software module and obtain second independent analysis (include the operating and maintenance department here and in all subsequent steps); thoroughly test the combination of modules that make up a process subsystem and obtain second independent analysis;
- thoroughly test the SIS application software;
- obtain second independent analysis;
- utilize application software when checking out the hardware (for example, confirming I/O connected to correct sensor/final element);
- include testing of the application software in the run-in (for example, process operation without hazardous material) of the process;
- application software support team members are to be available during process turnover to facility (for example, commissioning).

The application software documentation will be used to determine the suitability of the application software to each SIF SIL. An independent analysis should be made to determine that the application software meets the SIL.

IEC 61508-3 and IEC 61508-6 provide alternate approaches and further guidance in this matter.

12.4.2.1 No further guidance provided.

12.4.2.2 With regard to guidance on selection of application software design methods and techniques, systems with a safety requirement up to SIL 3 should be designed in accordance with the instructions given in the supplier's Safety Manual as part of a system conforming with IEC 61508. For SIL 4 systems, the developer should additionally confirm that the selected methods do conform with the requirements of IEC 61508-3.

With regard to guidance on selection of application software test and verification methods and techniques, systems with a safety requirement up to SIL 3 should be verified in accordance with the guidance given in 12.7. For SIL 4 systems, the verifier should also confirm that the selected methods do conform with the requirements of IEC 61508-3.

12.4.2.3 No further guidance provided.

12.4.2.4 In general, in order to ensure testability, it is recommended that the application software integration test specifications are considered during the design and development phase.

12.4.2.5 Where the application software in a SIS is to implement safety instrumented functions of different SILs, they should be clearly separated and labelled. This allows the software of each safety instrumented function to be traceable to the proper sensor and final element redundancy. It also allows the functional and validation testing of the functions to be commensurate with the SIL. The labelling should identify the SIF and the SIL.

Il convient que des zones séparées du logiciel soient utilisées pour les fonctions instrumentées non sécuritaires et pour les fonctions instrumentées de sécurité. Une manière de démontrer que l'indépendance idoine pourrait être de montrer que tous les points suivants sont remplis:

a) les fonctions instrumentées de sécurité dans le logiciel d'application sont clairement marquées en tant que code d'application de SIF;

b) les fonctions instrumentées non sécuritaires dans le logiciel d'application sont clairement séparées;

c) toutes les variables utilisées dans la mise en oeuvre des fonctions instrumentées de sécurité sont marquées;

d) tout le code de l'application mettant en oeuvre des fonctions instrumentées non sécuritaires est marqué en tant que code de fonction instrumentée non sécuritaire;

e) tout le code de l'application utilisant des variables non sécuritaires et des variables de SIF remplit les conditions suivantes:

   – le code de l'application non sécuritaire (programmes, fonctions et blocs fonctionnels) n'écrit dans aucune variable de SIF utilisée dans le code de l'application de sécurité;

   – le code de l'application de sécurité ne dépend d'aucune variable non sécuritaire dans la mise en œuvre des fonctions instrumentées de sécurité.

f) tout le logiciel d'application de sécurité (c'est-à-dire, code et variables) est protégé contre toutes les modifications du logiciel non sécuritaire;

g) Si le logiciel d'application de sécurité et le logiciel non sécuritaire partagent les mêmes ressources (par exemple, le CPU, les ressources du système d'exploitation, la mémoire, les bus), la fonction instrumentée de sécurité (par exemple, temps de réponse) du logiciel d'application de sécurité n'est alors jamais compromise.

Dans le meilleur des cas, il convient que les interactions entre le code de l'application (SIF et non sécuritaire) et toutes les variables (SIF et non sécuritaire) soient vérifiées automatiquement par le logiciel de développement de l'application. Si ce dispositif n'est pas disponible, il convient que le développeur du logiciel d'application et les autres personnes effectuant la vérification et la validation du logiciel d'application vérifient tout le code de l'application et les variables associées, pour garantir la conformité aux règles de séparation données ci-dessus.

12.4.2.6 Aucune ligne directrice n'est fournie.

12.4.2.7 Aucune ligne directrice n'est fournie.

12.4.3 Exigences relatives à l'architecture du logiciel d'application

Les variantes architecturales de logiciel possibles dans une unité logique de SIS typique sont très limitées et sont mieux comprises en examinant les étapes principales du développement des programmes d'application. Habituellement, le développeur réalisera les étapes principales suivantes lors du développement et des essais des programmes d'application:

a) configuration des modules d'E/S et des zones de données des variables en mémoire;

b) développement des noms d'étiquette pour toutes les E/S et les variables en mémoire. Il convient que les appellations des étiquettes suivent une convention cohérente;

c) définition de la technique de maintenance prioritaire. Certains utilisateurs exigeront des commutateurs câblés au niveau des points d'entrées numériques pour lancer la maintenance prioritaire. D'autres utiliseront des entrées de données contrôlées vers le SIS à partir d'une station d'affichage. Dans tous les cas, un traitement sécurisé doit être assuré pour éviter tout déclenchement fortuit. Il convient que les déclenchements de la maintenance prioritaire soient annoncés;

Separate areas of the software should be used for non-safety and safety instrumented functions. One way to demonstrate adequate independence could be to comply with all of the following:

a) safety instrumented functions in the application software are clearly labelled as SIF application code;

b) non safety instrumented functions in the application software are clearly separated;

c) all variables used in the implementation of safety instrumented functions are labelled;

d) all application code implementing non-safety-instrumented functions are labelled as non-safety instrumented function code;

e) all application code using non safety variables and SIF variables meet the following conditions:

   – the non safety application code (programs, functions and function blocks) do not write into any SIF variables used in the safety application code,

   – the safety application code does not depend on any non safety variables in the implementation of safety instrumented functions;

f) all safety application software (i.e., code and variables) is protected against any non-safety software changes;

g) if safety and non-safety application software share the same resources (for example, CPU, operating system resources, memory, buses), then the safety instrumented function (for example, response time) of the safety application software is never compromised.

Ideally, the interactions between the application code (SIF and non safety) and all variables (SIF and non safety) should be checked automatically by the application development software. If this feature is not available, the application software developer and other persons performing verification and validation of the application software should check all application code and associated variables for conformance to the separation rules given above.

12.4.2.6 No further guidance provided.

12.4.2.7 No further guidance provided.

12.4.3 Requirements for application software architecture

The software architectural variations possible in a typical SIS logic solver are very limited and are best understood by looking at the major steps in the development of the application programs. The developer will typically perform the following major steps in the development and testing of the application programs.

a) Configure the I/O modules and memory variable data areas.

b) Develop the tag names for all the I/O and memory variables. The tag naming should follow a consistent convention.

c) Define the technique for maintenance override. Some users will require switches wired through digital input points to initiate maintenance override. Others will use controlled data input to the SIS from a display station. In any case, secure handling has to be ensured to avoid unintended overrides. Maintenance overrides should be announced.

d) définition des diagnostics concernant le capteur et l'élément terminal, et philosophie des essais périodiques. Celle-ci dépendra de la redondance du capteur et de l'élément terminal. La philosophie nécessite d'être soigneusement définie et il convient qu'elle comprenne un dispositif d'alarme approprié pendant la période d'essai;

e) définition les variables de communication vers d'autres systèmes périphériques au SIS. Si les variables sont des variables destinées à être stockées en mémoire, elles devront être affectées aux zones de données appropriées, ainsi le sous-système de communication pourra y accéder. Il convient que les variables qui peuvent être modifiées par d'autres systèmes périphériques au SIS soient soigneusement définies et soient typiquement placées dans une zone spéciale de lecture/écriture de la mémoire;

f) définition d'où et comment la séquence d'événements est enregistrée et compréhension de son impact sur le SIS;

g) développement des fonctions personnalisées et des blocs fonctionnels. Cette personnalisation est très souhaitable puisque des opérations répétitives peuvent être programmées, essayées et utilisées à plusieurs reprises dans les programmes d'application;

NOTE Les fonctions, les blocs fonctionnels et les programmes sont définis dans la CEI 61131-3.

h) décision concernant le choix des fonctions instrumentées de sécurité et des autres fonctions qu'il convient d'inclure dans un programme donné. Il est souhaitable de séparer les fonctions de sécurité et non sécuritaires dans des programmes distincts, de sorte que l'accent puisse être mis sur les programmes critiques de sécurité. Il est également souhaitable de limiter la taille des programmes à quelques fonctions;

i) développement des programmes d'application. Il convient que la structure des programmes d'application soit conforme à la structure du processus. (Par exemple, il convient que dans une installation industrielle chimique les logiciels d'application pour chaque unité de processus soient regroupés). Au sein de chaque unité de processus, une séparation est prévue entre les équipements, pour faciliter la compréhension et la maintenance.

j) détermination de l'ordre d'exécution approprié des réseaux et de la logique, au sein de chaque programme et de la séquence d'exécution et des taux souhaités d'exécution de tous les programmes d'application. Confirmation que les taux d'exécution des programmes d'application sont cohérents avec les temps de réponse requis du processus, à partir de la spécification des exigences concernant la sécurité du logiciel;

k) essais du logiciel d'application en utilisant les possibilités de surveillance de l'environnement de développement (lorsqu'il est disponible);

l) téléchargement du logiciel d'application dans l'unité logique;

m) essais de toutes les entrées de l'unité logique, des sorties, du logiciel d'application et des interfaces vers les autres systèmes périphériques au SIS.

12.4.3.1 Aucune ligne directrice n'est fournie.

12.4.3.2 Aucune ligne directrice n'est fournie.

12.4.3.3 Aucune ligne directrice n'est fournie.

12.4.3.4 Aucune ligne directrice n'est fournie.

12.4.3.5 Des exemples de vérification d'intégrité des données de sécurité sont donnés ci-après:

– vérifications des données d'E/S hors gamme;

– validation des données d'application communiquées;

– vérifications de la cohérence des appellations des étiquettes, par exemple, vérifications de l'utilisation multiple des mêmes noms d'étiquette;

– vérifications de la validité des priorités, par exemple, vérifications de la priorité de la maintenance et de la mise en marche;

– vérification de validité des alarmes et des points de consigne.

d) Define the sensor and final element diagnostics and the periodic testing philosophy. This will be dependent on the sensor and final element redundancy. The philosophy needs to be defined carefully and should include the appropriate alarming during the test period.

e) Define the communication variables to other systems peripheral to the SIS. If the variables are memory variables they will have to be assigned to appropriate data areas so they can be accessed by the communication subsystem. Variables that can be modified by other systems peripheral to the SIS should be carefully defined and are typically placed in a special read/write area of memory.

f) Define where and how the sequence of events is recorded and understand its impact on the SIS.

g) Develop custom functions and function blocks. This customisation is very desirable since repetitive operations can be programmed, tested and used repeatedly in the application programs.

NOTE Functions, function blocks and programs are defined in IEC 61131-3.

h) Decide what safety instrumented functions and other functions should be included within a given program. It is desirable to separate the safety and non-safety functions into separate programs so that the emphasis can be placed on the safety critical programs. It is also desirable to limit the size of the programs to a few functions.

i) Develop the application programs. The application program structure should be consistent with the structure of the process. (for example, in a chemical plant the application software for each process unit should be grouped together. Within each process unit separation is provided between equipment for ease of understanding and maintenance).

j) Determine the proper execution order of the networks and logic, within each program and the execution sequence and desired execution rates of all the application programs. Confirm that the execution rates of the application programs are consistent with the required process response times from the software safety requirements specification.

k) Test the application software using the monitoring capability of the development environment (where available).

l) Download the application software into the logic solver.

m) Test all the logic solver inputs, outputs, application software and the interface to the other systems peripheral to the SIS.

12.4.3.1 No further guidance provided.

12.4.3.2 No further guidance provided.

12.4.3.3 No further guidance provided.

12.4.3.4 No further guidance provided.

12.4.3.5 Examples of safety data integrity verification include

- out of range I/O data checks;
- validation of communicated application data;
- tag naming consistency checks for example, multiple use of same tag name checks;
- override validity checks for example, maintenance and start-up override validity checks;
- alarm and set point validity check.

12.4.4 Exigences relatives aux outils supports, au manuel utilisateur et aux langages d'application

Un environnement de développement est un ensemble d'outils qui assiste le codage du logiciel d'application, de la configuration des paramètres de l'application et des interfaces, et des essais/de la surveillance de l'exécution du logiciel d'application. Habituellement, l'environnement offre les possibilités définies ci-dessous.

a) **Un éditeur de configuration.** Cet éditeur est utilisé pour configurer le sous-système d'E/S, les variables de mémoire d'E/S, et les fonctions de communication.

b) **Des éditeurs de langage.** Ces éditeurs sont utilisés par le programmeur de l'application pour développer les programmes qui exécutent toutes les fonctions requises par le système (de sécurité et non sécuritaire).

c) **Les bibliothèques des fonctions certifiées et des blocs fonctionnels.** Ces fonctions et blocs fonctionnels peuvent être utilisés dans les programmes d'application.

d) **Des possibilités de développement de fonction et de bloc fonctionnel personnalisés.** Certains fournisseurs proposent un environnement de développement qui permet à l'utilisateur de développer des fonctions et des blocs fonctionnels personnalisés, qui peuvent être utilisés par les langages de l'application, compatibles. Il convient que ces fonctions et ces blocs fonctionnels personnalisés soient complètement essayés avant leur utilisation dans le programme d'application.

e) **Une fonction d'ordonnancement du programme d'application.** Ces fonctions d'ordonnancement assistent l'établissement de l'ordre de la séquence d'exécution souhaitée et des taux de balayage.

f) **Des possibilités de téléchargement.** Ceci permet au développeur de télécharger le logiciel d'application, les bibliothèques de blocs fonctionnels, les données des variables et toutes autres informations de configuration dans le matériel de l'unité logique, pour exécution.

g) **Des possibilités d'émulation.** Certains fournisseurs proposent un environnement de développement avec des possibilités pour émuler tous les programmes d'application sur l'ordinateur qui supporte l'environnement de développement. Ceci permet d'effectuer des essais complets «hors ligne» des programmes d'application, avant qu'ils ne soient téléchargés dans l'unité logique.

h) **Des possibilités de surveillance de programme.** Les possibilités de surveillance permettent à l'utilisateur de visualiser des données du programme d'exécution sur des écrans définis par l'utilisateur ou sur des écrans de programme en langage en bloc fonctionnel réel ou en langage à contacts. L'environnement de développement peut également offrir des possibilités pour surveiller l'exécution de l'émulateur. En plus, les programmes s'exécutant dans l'unité logique peuvent être surveillés.

i) **Des affichages de diagnostic de l'unité logique.** Ces affichages présentent l'état des modules processeur principaux, des modules de communication, et des modules d'E/S dans le système. Typiquement les états actifs «bon», «mauvais», de chaque module sont présentés, et dans de nombreux cas, des informations plus détaillées sur les anomalies au sein du système sont disponibles.

12.4.4.1 Aucune ligne directrice n'est fournie.

12.4.4.2 Aucune ligne directrice n'est fournie.

12.4.4.3 Aucune ligne directrice n'est fournie.

12.4.4.4 La préférence va aux traducteurs de langage d'application, qui sont éprouvés en utilisation et/ou ont été certifiés par rapport à des normes industrielles reconnues.

12.4.4.5 Aucune ligne directrice n'est fournie.

12.4.4 Requirements for support tools, user manual and application languages

A development environment is a set of tools which supports the coding of the application software, the configuration of application parameters and interfaces and the testing/ monitoring of the application software execution. The environment typically provides the following capabilities.

a) **Configuration editor.** This editor is used to configure the I/O subsystem, the I/O memory variables, and communication functions.

b) **Language editors.** These editors are used by the application programmer to develop the programs that perform all the functions needed by the system (safety and non-safety).

c) **Libraries of certified functions and function blocks.** These functions and function blocks can be used in the application programs.

d) **Custom function and function block development capability.** Some suppliers provide a development environment that allows the user to develop custom functions and function blocks that can be used by the supported application languages. These custom functions and function blocks should be thoroughly tested prior to use in the application program.

e) **Application program scheduling facility.** These scheduling facilities support the setting of the order of desired execution sequence and their scan rates.

f) **Downloading capability.** This allows the developer to download the application software, function block libraries, variable data and other configuration information into the logic solver hardware for execution.

g) **Emulation capability.** Some suppliers provide a development environment with the capability to emulate all of the application programs on the computer that supports the development environment. This allows thorough off-line testing of the application programs before they are downloaded into the logic solver.

h) **Program monitoring capability.** The monitoring capability allows the user to view data from the executing program on user-defined screens or on the actual function block or ladder diagram program screens. The development environment may also provide the capability to monitor the execution of the emulator. In addition, the programs executing in the logic solver can be monitored.

i) **Diagnostic displays of the logic solver.** These displays show the status of the main processor modules, communication modules, and the I/O modules in the system. Typically, the pass, fail, active status of each module is shown; and in many cases, more detailed information about faults in the system is available.

12.4.4.1 No further guidance provided.

12.4.4.2 No further guidance provided.

12.4.4.3 No further guidance provided.

12.4.4.4 Application language translators that are proven in use and/or have been certified to accepted industry standards are preferred.

12.4.4.5 No further guidance provided.

12.4.4.6 Aucune ligne directrice n'est fournie.

12.4.4.7 Exemple de Manuel de sécurité

Il convient que les composants et les dispositifs utilisés dans les applications de SIF conformes à cette norme soient livrés avec une documentation donnant le détail de tous les aspects connus de l'installation, de la maintenance, de la configuration, de la programmation et de l'exploitation; il convient que ces aspects soient respectés, si le composant ou le dispositif doit répondre à la spécification des exigences concernant la sécurité de l'application.

Ce document est fréquemment intitulé «Manuel de sécurité» du composant ou du dispositif. Il peut, cependant, être composé des manuels standards des fournisseurs d'installation, de maintenance et de l'utilisateur, avec un document additionnel spécifiant les aspects concernant son utilisation dans les applications de SIF, les limitations d'utilisation dans ces applications, les actions qu'il convient d'entreprendre au sujet des alarmes de diagnostic et des modes de défaillance connus. Il convient également de définir ces fonctionnalités, configurations et/ou types d'instruction de programme qu'il convient de ne pas employer lorsque le composant ou le dispositif est utilisé dans une application de SIF.

La programmation de variabilité limitée permet l'utilisation de données globales; donc, il convient que le Manuel de sécurité donne des directives au programmeur sur la façon dont il doit utiliser les outils de programmation pour examiner en détail et vérifier l'utilisation correcte des variables de données. Les autres fonctionnalités à traiter peuvent comprendre le cartographie mémoire, des vérifications sur des drapeaux d'état et des vérifications de validité sur des valeurs d'entrée.

Les instructions et les exemples pour permettre à un groupe de programmeurs de produire des programmes de format et de style similaires peuvent également être proposés comme faisant partie du manuel de sécurité ou comme un document spécifique à l'application. Il convient que ces instructions incluent les détails des algorithmes spécifiques ou des fonctions qui ne sont pas à utiliser dans les programmes, puisque ces algorithmes ou ces fonctions peuvent avoir comme conséquence un comportement non prévu, qui pourrait affecter la sécurité.

Il convient que le programmeur soit mis en garde de ne pas faire d'hypothèse, en dehors de celles définies par le manuel de sécurité, par exemple, ne pas utiliser les possibilités d'un compilateur qui ne seraient pas mentionnées dans le manuel de sécurité. Dans le meilleur des cas, le compilateur aura été configuré pour imposer ces restrictions.

Exemple de plan et de sommaire de manuel de sécurité

Le plan d'organisation de manuel, accompagné d’un exemple de sommaire, qui est donné dans le Tableau 1 est prévu pour une unité logique typique qui satisfait à la CEI 61511.

L'exemple donne la liste de tous les chapitres, en indiquant, pour chacun, les en-têtes des principaux contenus.

12.4.4.6 No further guidance provided.

12.4.4.7 Safety Manual example

Components and devices used in SIF applications that comply with this standard should be provided with documentation that details all known aspects of installation, maintenance, configuration, programming and operation that should be observed if the component or device is to meet the safety requirements specification of the application.

This standard is frequently titled the “Safety Manual” of the component or device. It may, however, be comprised of the suppliers standard Installation, Maintenance and User’s Manuals with an additional document specifying those aspects relating to its use in SIF applications, the limitations of use in these applications, the actions that should be taken on diagnostic alarms and the known failure modes. It should also define those features, configurations and/or program statement types that should not be used when the component or device is used in a SIF application.

Limited variability programming allows the use of global data; therefore, the Safety Manual should provide guidance to the programmer on how to use the programming tools to scrutinise and check the correct use of data variables. Other features to address may include memory mapping, checks on status flags and validity checks on input values.

Instructions and examples to enable a group of programmers to produce programs of similar format and style may also be provided either as part of the Safety Manual or as an application specific document. These instructions should include details of specific algorithms or functions that are not to be used in the programs, since the algorithms or functions may result in unexpected behaviour which might affect safety.

The programmer should be warned not to make any assumptions beyond those defined in the Safety Manual, for example, not to use compiler capabilities which are omitted from the Safety Manual. Ideally, the compiler would have been configured to enforce these restrictions.

Example of a typical Safety Manual organization and contents

The following example of a manual organization diagram with contents example is for a typical logic solver that conforms to IEC 61511.

The example shows each individual chapter with the primary contents headings for each chapter shown.

Tableau 1 – Organisation et contenu d'un manuel de sécurité type

Chapitres	Principal contenu
Introduction	Informations générales, exigences des équipements, organisation du manuel, conventions, documentation connexe, historique des mises à jour, terminologie, vue d'ensemble du produit.
Installation	Environnement de planification du site, connexions au processus, procédures de mise en marche, procédures d'arrêt, modifications de l'application, mise en œuvre des fonctions dans des systèmes déjà en exploitation.
Configuration et construction de l'application	*Considérations de conception, capacité et performances, didacticiel.
Exploitation/Fonctionnement	Fonctionnement du produit, vue d'ensemble de l'exploitation, instructions d'exploitation.
Maintenance	Maintenance préventive, indicateurs matériels, messages d'erreur, alarmes de l'application et du système, recherche d'anomalie et réparation utilisateur.
Annexes	Messages système, liste des vérifications, solutions de l'application.
Index	Index des messages de sécurité.

* Les considérations de conception spécifient tous les aspects de la configuration et de la programmation de l'application, appropriés à une configuration et à une programmation sûres de l'unité logique à électronique programmable (PE). Celles-ci incluront de manière non exhaustive:

- Les temps de traitement de l'unité logique, les taux de mise à jour des E/S, les taux de communication, la séquence des opérations de l'unité logique;
- Les exigences de traitement des alarmes du système;
- Les contraintes de configuration et de programmation.

12.4.4.8 Aucune ligne directrice n'est fournie.

12.4.5 Exigences relatives au développement du logiciel d'application

Avant d'entreprendre le développement du logiciel d'application, il convient de vérifier les points suivants:

– il convient que l'unité logique du SIS et ses modules d'E/S associés soient en conformité avec la CEI 61511-1;

– il convient que toutes les restrictions et les procédures opérationnelles nécessaires pour montrer la conformité à la CEI 61511-1 soient données par la documentation utilisateur ou par les documents édités par le fournisseur de l'unité logique. Ces documents sont généralement désignés par le nom de «Manuel de sécurité»;

– il convient que les capteurs et les éléments terminaux utilisant une électronique programmable soient en conformité avec la CEI 61511;

– Lorsque des essais périodiques «en ligne» sont réalisés, une possibilité de maintenance prioritaire peut être offerte pour permettre les essais des capteurs et des éléments terminaux.

Le logiciel d'application est habituellement écrit dans des langages de programmation proposés par le fournisseur de l'unité logique ou par les fournisseurs des dispositifs de terrain intelligents. L'application peut être écrite en utilisant un langage de variabilité totale (FVL), comme une liste d'instructions ou le C, un langage de variabilité limitée (LVL), comme le langage en blocs fonctionnels ou le langage à contacts, ou un langage de programme figé (FPL) où l'utilisateur ne peut saisir que les données requises par le programme figé.

Si le logiciel d'application est écrit en FVL, il convient que le développeur suive les exigences et les directives de la CEI 61508. Si le logiciel d'application est écrit en LVL ou en FPL, le développeur peut suivre les exigences et les directives de la CEI 61511. Il convient que le développeur suive les restrictions et les procédures données par le fournisseur de l'unité logique, incluses dans le manuel de sécurité. Il convient que les directives de programmation et les règles de codage/de configuration soient également développées et utilisées, si nécessaires.

Table 1 – Typical Safety Manual organisation and contents

Chapters	Principal contents
Introduction	General information, equipment requirements, manual organization, conventions, related documentation, release history, terminology, product overview.
Installation	Site planning environment, process connections, start-up procedures, shut-down procedures, application modifications, implementation of functions in systems already operating.
Configuration and application building	Design considerations[a], capacity and performance, tutorial
Runtime operation	Product operation, operating overview, operating instructions
Maintenance	Preventive maintenance, hardware indicators, error messages, application and system alarms, fault finding and user repair
Appendices	System messages, check list, application solutions
Index	Safety message index

[a] Design considerations specify all aspects of configuration and application programming that are relevant to the safe configuration and programming of the PE logic solver. These will include but not be limited to:
- logic solver processing times, I/O update rates, communication rates, sequence of logic solver operations;
- system alarm handling requirements;
- constraints of configuration and programming.

12.4.4.8 No further guidance provided.

12.4.5 Requirements for application software development

Before proceeding with the development of the application software, the following items should be checked:

- the SIS logic solver and its associated I/O modules should be in compliance with IEC 61511-1;
- all restrictions and operating procedures necessary for compliance with IEC 61511-1 should be provided in user documentation or documents issued by the logic solver vendor. These documents are commonly referred to as the Safety Manual;
- sensors and final elements utilising programmable electronics should be in compliance with IEC 61511-1;
- when periodic on-line testing is performed, a maintenance override capability may be provided to allow testing of sensors and final elements.

The application software is typically written in the programming languages provided by the logic solver supplier or the smart field device suppliers. The application can be written using a full variability language (FVL) such as instruction list or C, a limited variability language (LVL) such as function block diagram or ladder diagram, or a fixed program language (FPL) where the user only enters data needed by the fixed program.

If the application software is written in a FVL, the developer should follow the requirements and guidelines in IEC 61508-3. If the application software is written in LVL or FPL, the developer may follow the IEC 61511-1 requirements and guidelines. The developer should follow the restrictions and procedures provided by the logic solver vendor in the Safety Manual. Programming guidelines and coding/configuration rules should also be developed and used if needed.

12.4.5.1 Aucune ligne directrice n'est fournie.

12.4.5.2 Aucune ligne directrice n'est fournie.

12.4.5.3 Un exemple d'une variable globale de l'application serait une alarme de sécurité, telle qu'une alarme de haute température, qui est modifiée en fonction des constituants des lots, objets du processus.

Un exemple d'une constante globale de l'application serait la limite d'alarme d'un gaz hautement combustible utilisé dans les systèmes de protection contre l'incendie et les gaz, par exemple, 20 % LEL (Lower Explosion Limit = limite inférieure d'explosion).

12.4.5.4 Aucune ligne directrice n'est fournie.

12.4.5.5 Aucune ligne directrice n'est fournie.

12.4.5.6 Aucune ligne directrice n'est fournie.

12.4.6 Exigences relatives aux essais des modules logiciels de l'application

Les essais du logiciel d'application peuvent avoir lieu initialement sur un simulateur et ensuite sur le matériel de l'unité logique en s'appuyant sur les spécifications produites lors des étapes de conception et de spécification des exigences. Le but des phases d'essai initiales (simulation et essais par rapport aux spécifications de conception) est:

– de démontrer que les modules logiciels apportent la fonctionnalité nécessaire et sont incapables de tout comportement interdit;
– de soumettre le logiciel à une large gamme de conditions et de séquences pour démontrer qu'il résiste à un comportement imprévu.

Le but des étapes d'essais suivantes (essai d'intégration et essais de recette en usine [FAT]) est de démontrer que le logiciel d'application rempli ses exigences, au sein du matériel spécifié et dans les conditions temporelles définies.

L'étape finale des essais, c'est-à-dire, la démonstration que le système intégré fonctionne correctement dans son environnement prévu, avec les dispositifs physiques et les interfaces prévus et avec les procédures opérationnelles définies, ne peut être entièrement réalisée que pendant l'installation et la mise en service de l'ensemble du système.

Dès le début des essais formels, il convient que toutes les modifications aux fonctions du logiciel et à la configuration des données soient mises en application de manière stricte, en accord avec une procédure de modification définie.

12.4.6.1 Aucune ligne directrice n'est fournie.

12.4.6.2 Aucune ligne directrice n'est fournie.

12.4.6.3 Aucune ligne directrice n'est fournie.

12.4.7 Exigences relatives aux essais d'intégration du logiciel d'application

12.4.7.1 Aucune ligne directrice n'est fournie.

12.4.7.2 Aucune ligne directrice n'est fournie.

12.4.7.3 Aucune ligne directrice n'est fournie.

12.4.5.1 No further guidance provided.

12.4.5.2 No further guidance provided.

12.4.5.3 An example of an application global variable would be a safety alarm such as a high temperature alarm that is changed depending on the batch constituents under process.

An example of an application global constant would be the high combustible gas alarm limit used in fire and gas protection systems, for example, 20 % LEL (Lower Explosion Limit).

12.4.5.4 No further guidance provided.

12.4.5.5 No further guidance provided.

12.4.5.6 No further guidance provided.

12.4.6 Requirements for application software module testing

Application software testing may take place initially on a simulator and then on the logic solver hardware against the specifications produced in the design and requirements specification stages. The purpose of the initial testing phases (simulation and testing against the design specifications) is:

- to demonstrate that the software modules provided the necessary functionality and are incapable of any prohibited behaviour;
- to subject the software to a wide range of conditions and sequences to show that it is resilient to unexpected behaviour.

The purpose of subsequent stages of testing (integration test and factory acceptance test) are to show that the application software achieved its requirements on the specified hardware and within the defined time relationships.

The final stage of testing, i.e., demonstration that the integrated system worked correctly in its intended environment, with the intended physical devices and interfaces and with the defined operating procedures, can only be fully completed during the whole system installation and commissioning.

From the start of the formal testing, all changes to software functions and configuration data should be implemented strictly in accordance with a defined modification procedure.

12.4.6.1 No further guidance provided.

12.4.6.2 No further guidance provided.

12.4.6.3 No further guidance provided.

12.4.7 Requirements for application software integration testing

12.4.7.1 No further guidance provided.

12.4.7.2 No further guidance provided.

12.4.7.3 No further guidance provided.

12.5 Intégration du logiciel d'application avec le sous-système du SIS

12.5.1 Objectif

12.5.1.1 Aucune ligne directrice n'est fournie.

12.5.2 Exigences

12.5.2.1 L'essai d'intégration peut être mis en oeuvre à n'importe quelle phase, jusqu'à l'étape de validation du SIS.

12.5.2.2 Aucune ligne directrice n'est fournie.

12.5.2.3 Aucune ligne directrice n'est fournie.

12.6 Procédures de modification du logiciel utilisant le FPL et le LVL

12.6.1 Objectif

12.6.1.1 Aucune ligne directrice n'est fournie.

12.6.2 Exigences de modification

Dans la mesure du possible, il convient d'éviter les modifications «en ligne» sur un système instrumenté de sécurité. Si des modifications «en ligne» sont requises, il convient de documenter la procédure complète et de l'approuver, en accord avec la planification de sécurité.

Le processus suivant est recommandé pour toutes les modifications aux systèmes instrumentés de sécurité programmables.

a) Planification et ressources

   Pour modifier un système instrumenté de sécurité programmable, il convient qu'un programme, soit géré, planifié et comporte des ressources au niveau approprié pour assurer la mise en œuvre des modifications en toute sécurité.

b) Analyse d'impact

   La modification requise peut nécessiter une analyse complète de danger et de risque, comprenant tous les effets possibles sur les parties non modifiées du système (analyse d'impact sur la sécurité).

c) Conception

   Il convient que la conception de la modification suive le processus de cycle de vie complet comme cela est décrit par la CEI 61511–1.

d) Vérification

   Il convient qu'une vérification complète «hors-ligne» du matériel et du logiciel d'application, soit effectuée avant l'installation de la modification.

   Dans le cas où la frontière des modifications du logiciel pourrait être clairement délimitée et maîtrisée, seul le logiciel d'application ainsi délimité nécessiterait d'être vérifié devant la mise en service.

e) Installation et mise en service

   Il convient que l'installation et la mise en service de la modification suivent les procédures définies par la CEI 61511–1 concernant l'installation et la mise en service des systèmes instrumentés de sécurité.

f) Validation des essais de recette

   Une validation du système (essai de cause à effet) sera mise en oeuvre pour les parties modifiées des systèmes, avant de mettre «en ligne» les parties modifiées du système.

12.5 Integration of the application software with the SIS subsystem

12.5.1 Objective

12.5.1.1 No further guidance provided.

12.5.2 Requirements

12.5.2.1 The integration test may be implemented at any phase up to the SIS validation.

12.5.2.2 No further guidance provided.

12.5.2.3 No further guidance provided.

12.6 FPL and LVL software modification procedures

12.6.1 Objective

12.6.1.1 No further guidance provided.

12.6.2 Modification requirements

Wherever possible, on-line modifications to a safety instrumented system should be avoided. If on-line modifications are required, the complete procedure should be documented and approved according to the safety planning.

The following process is recommended for all changes to programmable safety instrumented systems:

a) Planning and resources

A program to modify a programmable safety instrumented system should be managed, planned and resourced to the appropriate level to ensure the safe implementation of the change.

b) Impact analysis

The required modification may require a full hazard and risk assessment including all possible effects on the unchanged parts of the system (safety impact analysis).

c) Design

The modification design should follow the full lifecycle process as described in IEC 61511–1.

d) Verification

Full offline verification for hardware and application software should be completed prior to the installation of the change.

Where the boundary of the software changes can be clearly delineated and controlled, only the delineated application software needs to be verified before commissioning.

e) Installation and commissioning

The installation and commissioning of the change should follow the procedures defined in IEC 61511–1 for installation and commissioning of safety instrumented systems.

f) Acceptance test validation

A system validation (cause and effect test) will be implemented for the modified parts of the systems prior to bringing the modified parts of the system online.

g) Personnel

Il convient que seules les personnes désignées, qualifiées pour mettre en oeuvre les modifications et dont la compétence est basée sur leur formation et leur expertise, soient autorisées à effectuer les modifications.

h) Modifications «hors-ligne»

Lors de la mise en application des modifications «hors-ligne» du logiciel d'application, il convient de vérifier que les versions correctes du logiciel d'application sont utilisées, y compris celles des paramètres opérationnels.

12.6.2.1 Aucune ligne directrice n'est fournie.

12.7 Vérification du logiciel d'application

12.7.1 Objectifs

12.7.1.1 Aucune ligne directrice n'est fournie.

12.7.1.2 Aucune ligne directrice n'est fournie.

12.7.2 Exigences

La spécification de exigences concernant la sécurité du logiciel d'application comprendra:

– les exigences des fonctions instrumentées de sécurité (par exemple, les SIL des fonctions instrumentées de sécurité, organigrammes logiques/les diagrammes de cause et d'effet);
– les contraintes de synchronisation (par exemple, temps de réponse minimal des entrées vers les sorties);
– les contraintes architecturales (par exemple, exigences de redondance, interfaces de communication, ségrégation fonctionnelle).

La vérification garantit que les exigences spécifiées sont tenues à chaque phase du développement du logiciel d'application.

La vérification des données inclut la confirmation que les données utilisées dans le logiciel d'application sont correctes et uniques, le cas échéant (par exemple que les noms d'ETIQUETTE sont affectés de manière unique, que les données ne sont pas mal utilisées par les fonctions suivantes et que les constantes, tels que des points de consigne d'alarme, sont valides et correctes).

La vérification de la protection contre une modification non autorisée pourrait inclure la vérification que les mécanismes existent bien (par exemple, protection par mot de passe avec des niveaux d'accès) et que ces mécanismes ont été utilisés de manière adéquate.

12.7.2.1 Aucune ligne directrice n'est fournie.

12.7.2.2 Aucune ligne directrice n'est fournie.

12.7.2.3 A chaque phase distincte du cycle de développement du logiciel d'application (essais y compris), la vérification confirme que la phase a été terminée avec succès. En général, la vérification est accomplie par une équipe de vérification qui se compose d'une ou de plusieurs personnes.

Pour réduire des erreurs dues aux idées préconçues, il convient que la vérification comporte:

– pour le SIL 1, un examen critique par un autre membre de l'équipe de développement de l'application;

g) Personnel

Only identified personnel who are competent to implement modifications based on their training and expertise should be authorised to carry out modifications.

h) Off-line modifications

When implementing off-line modifications of the application software, it should be verified that the correct versions of the application software, including operational parameters, are used.

12.6.2.1 No further guidance provided.

12.7 Application software verification

12.7.1 Objectives

12.7.1.1 No further guidance provided.

12.7.1.2 No further guidance provided.

12.7.2 Requirements

The application software safety requirements specification will include:

- the safety instrumented function requirements (for example, SIL's of safety instrumented functions; logic flow diagrams/cause and effect diagrams);
- timing constraints (for example, input to output minimum response times);
- architectural constraints (for example, redundancy requirements, communication interfaces and functional segregation).

Verification ensures that the specified requirements are being met at each phase of the application software development.

Data verification includes confirmation that data used within the application software is correct and where appropriate unique (for example that TAG names are uniquely assigned, that data is not misused by subsequent functions and that constants such as alarm set points are valid and correct).

Verification for protection against unauthorised change, would include verification that the mechanisms exist (for example, password protection with levels of access) and that these mechanisms have been adequately utilised.

12.7.2.1 No further guidance provided.

12.7.2.2 No further guidance provided.

12.7.2.3 At each distinct phase of the application software development cycle (including testing), verification confirms that the phase has been successfully completed. Verification is, in general, completed by a verification team that consists of one or more persons.

To reduce errors due to preconceived mindsets, the verification should include:

- for SIL 1, a peer review by another member of the application development team;

– pour le SIL 2, un examen critique par une personne qui n'est pas membre de l'équipe de développement de l'application;
– pour le SIL 3, un examen critique par une personne qui est membre d'un département/service indépendant;

Dans le cas où les outils de développement du logiciel incluraient certaines opérations de vérification automatiques (par exemple, la vérification d'une double utilisation d'étiquettes (variables nommées)), il conviendrait alors que l'équipe de vérification confirme que les outils ont été correctement utilisés et que des résultats corrects ont été obtenus.

Pour tous les SIL, il est recommandé que la couverture des essais englobe toutes les réponses des SIF du logiciel d'application et du SIS aux défaillances (par exemple, défaillances de l'alimentation en énergie, défaillance du processeur, défaillance matérielle d'une entrée, défaillance matérielle d'une sortie et défaillances de communication). Toutefois pour réduire encore davantage les erreurs restantes du logiciel, pour les SIL les plus élevés, il est recommandé d'effectuer les essais supplémentaires suivants:

– pour le SIL 2 et pour le SIL 3, essais basés sur la structure interne (par exemple, algorithmes internes, états internes);
– pour le SIL 3, essais aux limites (par exemple, conditions de plage anormale des variables d'entrée et des variables internes, combinaisons anormales des entrées, séquences anormales et chargements anormaux).

Pour tous les SIL, il est recommandé de faire en sorte que la documentation de vérification et d'essai soit suffisante pour montrer que la vérification et les essais ont été effectués avec succès. Cependant, pour les SIL les plus élevés, il est recommandé également,

– pour le SIL 2 et pour le SIL 3, que la documentation soit suffisante pour permettre une évaluation de l'adéquation de la vérification et des essais;

  pour le SIL 3, qu'il convient que la documentation soit suffisante pour permettre à une personne indépendante de répéter les essais et d'examiner la couverture obtenue.

12.7.2.4 Aucune ligne directrice n'est fournie.

13 Essais de recette en usine (FAT)

13.1 Objectifs

13.1.1 Aucune ligne directrice n'est fournie.

13.2 Recommandations

13.2.1 Bien que la conduite des essais de recette en usine (FAT) ne soit pas une prescription, ces derniers sont recommandés pour les unités logiques mettant en œuvre des fonctions instrumentées de sécurité ayant une logique d'application assez complexe ou des configurations de redondance (par exemple, 1oo2, 1oo2D, 2oo3 etc.).

13.2.2 Le point le plus important des FAT est d'avoir une procédure d'essai bien définie, bien écrite et bien structurée, qui définit comment essayer la logique de l'application et ce qu'il y a à rechercher après chaque étape.

Il convient que le personnel qui exploitera le processus assiste aux FAT, car il donnera une formation préalable sur l'exploitation du SIS. Fréquemment, il peut également proposer de bonnes suggestions ou des perfectionnements intéressants à la procédure d'essai, qui n'ont pas été prévus pendant la conception.

13.2.3 Aucune ligne directrice n'est fournie.

- for SIL 2, a peer review by a person who is not a member of the application development team;
- for SIL 3, a peer review by a person who is a member of an independent department.

Where the software development tools include some automatic verification operations (for example, checking for double use of tags (named variables)) then the verification team should confirm that the tools have been properly used and the correct results obtained.

For all SILs, it is recommended that the test coverage encompasses all application software SIFs and SIS failure responses (for example, power supply failures, processor failure, input hardware failure, output hardware failure and communication failures). However to further reduce any errors remaining in the software, for higher SILs it is recommended that the following additional testing is carried out:

- for SIL 2 and SIL 3, testing based on the internal structure (for example, internal algorithms, internal states);
- for SIL 3, stress testing (for example, abnormal range conditions of input variables and internal variables, abnormal combinations of inputs, abnormal sequences and loading).

For all SILs it is recommended that the verification and test documentation is sufficient to show that the verification and tests have been carried out and were successful. However, for higher SILs, it is also recommended that:

- for SIL 2 and SIL 3, the documentation is sufficient to allow an assessment of the adequacy of the verification and testing;
- for SIL 3, the documentation should be sufficient to allow an independent person to repeat the tests and review the coverage achieved.

12.7.2.4 No further guidance provided.

13 Factory acceptance testing (FAT)

13.1 Objectives

13.1.1 No further guidance provided.

13.2 Recommendations

13.2.1 Although conducting a Factory Acceptance Test (FAT) is not a requirement, a FAT is recommended for those logic solvers implementing safety instrumented functions having fairly complex application logic or redundancy arrangements (for example, 1oo2, 1oo2D, 2oo3 etc.).

13.2.2 The most important part of the FAT is to have a well defined, well written and well structured test procedure that defines how to test the application logic and what to look for after each step.

Personnel that will be operating the process should attend the FAT since it will give them some early training on the operation of their SIS. Often, they can also provide good suggestions or enhancements to the test procedure that were not foreseen during the design.

13.2.3 No further guidance provided.

13.2.4 Aucune ligne directrice n'est fournie.

13.2.5 Pendant les FAT, il convient que les interfaces soient essayées (par exemple, les communications entre le BPCS et le SIS).

13.2.6 Aucune ligne directrice n'est fournie.

13.2.7 Aucune ligne directrice n'est fournie.

14 Installation et mise en service du SIS

14.1 Objectifs

14.1.1 Aucune ligne directrice n'est fournie.

14.2 Exigences

14.2.1 Aucune ligne directrice n'est fournie.

14.2.2 Il convient que le SIS soit installé conformément au plan de conception et d'installation. Il convient de passer correctement en revue, avec l'équipe de projet, tous les écarts par rapport à la conception, pour s'assurer que toutes les exigences de conception sont toujours satisfaites. Après avoir correctement installé le SIS, il convient de le mettre en service entièrement et de lancer les activités de validation.

14.2.3 Alors que la CEI 61511-1 a traité la mise en service comme une phase unique, il est reconnu que l'application, l'expérience de l'équipe de projet, et les nécessités du projet, peuvent demander que la mise en service soit réalisée en plusieurs phases.

14.2.4 Aucune ligne directrice n'est fournie.

14.2.5 Aucune ligne directrice n'est fournie.

15 Validation de sécurité du SIS

15.1 Objectif

15.1.1 L'objectif de la validation de sécurité du SIS est de prouver que le SIS remplit les exigences indiquées dans la spécification des exigences concernant la sécurité. Il convient que les activités de validation soient achevées avant de mettre le SIS en l'exploitation.

15.2 Exigences

15.2.1 Aucune ligne directrice n'est fournie.

15.2.2 Aucune ligne directrice n'est fournie.

15.2.3 Aucune ligne directrice n'est fournie.

15.2.4 Si le SIS a déjà été soumis à des essais de recette en usine (FAT), ceux-ci peuvent être pris en compte lors de la validation. Il convient que l'équipe de validation examine finement les résultats des FAT, pour s'assurer que tout le logiciel d'application a été essayé avec succès et que tous les problèmes trouvés pendant les FAT ont été corrigés.

13.2.4 No further guidance provided.

13.2.5 During the FAT, interfaces should be tested (for example, communications between the BPCS and SIS).

13.2.6 No further guidance provided.

13.2.7 No further guidance provided.

14 SIS installation and commissioning

14.1 Objectives

14.1.1 No further guidance provided.

14.2 Requirements

14.2.1 No further guidance provided.

14.2.2 The SIS should be installed per the design and installation plan. Any deviations from the design should be properly reviewed with the project team to ensure all of the design requirements are still satisfied. After the SIS has been properly installed, it should be fully commissioned and validation activities should be initiated.

14.2.3 While IEC 61511-1 has addressed commissioning as a single phase, it is recognized that the application, the experiences of the project team, and project needs may require commissioning to be accomplished in several phases.

14.2.4 No further guidance provided.

14.2.5 No further guidance provided.

15 SIS safety validation

15.1 Objective

15.1.1 The objective of the SIS safety validation is to validate that the SIS achieves the requirements stated in the safety requirements specification. Validation activities should be completed prior to the placing of the SIS into operation.

15.2 Requirements

15.2.1 No further guidance provided.

15.2.2 No further guidance provided.

15.2.3 No further guidance provided.

15.2.4 If the SIS has already been through a Factory Acceptance Test (FAT), this may be taken into consideration during the validation. The validation team should review the results of the FAT to ensure that all of the application software was successfully tested and all problems found during the FAT have been corrected.

Il peut être inutile de répéter les essais du logiciel d'application lors de la validation finale. Ceci est applicable lorsque:

– cette approche a été prévue et incluse dans la planification de la validation;
– le logiciel d'application a été vérifié pour satisfaire à la spécification des exigences concernant la sécurité pendant les FAT; et
– il est vérifié que la version du logiciel d'application est identique à la version essayée lors des FAT.

Cependant, il sera très important de s'assurer qu'il n'y a eu aucun dommage d'expédition/de stockage/de manipulation, que tous les capteurs et éléments terminaux sont correctement connectés à l'unité logique, que les fonctions instrumentées de sécurité fonctionnent correctement et que l'interface opérateur fournit les informations nécessaires. L'équivalent d'un test périodique est vivement recommandé afin de revendiquer la validation du SIS, du fait qu'un essai séparé de l'unité logique et des éléments de terrain n'est pas identique à un test périodique complet de bout-en-bout.

15.2.5 Aucune ligne directrice n'est fournie.

15.2.6 Aucune ligne directrice n'est fournie.

15.2.7 Aucune ligne directrice n'est fournie.

15.2.8 Aucune ligne directrice n'est fournie.

16 Exploitation et maintenance du SIS

16.1 Objectifs

16.1.1 Aucune ligne directrice n'est fournie.

16.2 Exigences

16.2.1 Aucune ligne directrice n'est fournie.

16.2.2 Aucune ligne directrice n'est fournie.

16.2.3 Aucune ligne directrice n'est fournie.

16.2.4 Aucune ligne directrice n'est fournie.

16.2.5 Aucune ligne directrice n'est fournie.

16.2.6 Aucune ligne directrice n'est fournie.

16.2.7 Aucune ligne directrice n'est fournie.

16.2.8 Aucune ligne directrice n'est fournie.

16.3 Tests périodiques et inspection

16.3.1 Tests périodiques

16.3.1.1 Il convient que l'intervalle des tests périodiques soit choisi pour obtenir la probabilité moyenne des défaillances sur sollicitation comme cela est demandé par la spécification des exigences concernant la sécurité.

16.3.1.2 Aucune ligne directrice n'est fournie.

It may be unnecessary to repeat application software testing at the final validation. This is applicable when

- this approach was anticipated and included in the validation planning,
- the application software has been verified to meet the safety requirements specification during the FAT, and
- the application software version is verified to be the identical version tested at the FAT.

However, it will be very important to ensure that there has been no shipping/storage/handling damage, that all sensors and final elements are correctly connected to the logic solver, that the safety instrumented functions perform properly and that the operator interface provides the necessary information. The equivalent of a proof test is strongly recommended in order to claim SIS validation, because a separate test of the logic solver and the field elements does not equal a complete end-to-end proof test.

15.2.5 No further guidance provided.

15.2.6 No further guidance provided.

15.2.7 No further guidance provided.

15.2.8 No further guidance provided.

16 SIS operation and maintenance

16.1 Objectives

No further guidance provided.

16.2 Requirements

16.2.1 No further guidance provided.

16.2.2 No further guidance provided.

16.2.3 No further guidance provided.

16.2.4 No further guidance provided.

16.2.5 No further guidance provided.

16.2.6 No further guidance provided.

16.2.7 No further guidance provided.

16.2.8 No further guidance provided.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 The proof test interval should be selected to achieve the average probability of failure on demand as required in the safety requirements specification.

16.3.1.2 No further guidance provided.

16.3.1.3 Il convient que la fréquence des tests périodiques soit cohérente avec les recommandations applicables du constructeur et avec les bonnes pratiques en matière d'ingénierie, et plus fréquemment, s'il est déterminé que cela est nécessaire, par une expérience d'exploitation antérieure.

Un certain nombre de stratégies sont à utiliser pour choisir l'intervalle des tests périodiques pour un SIF.

Par exemple, certains utilisateurs aiment choisir cet intervalle de tests périodiques aussi long que possible, pour minimiser le coût de maintenance et l'impact potentiel des essais. Dans ce cas, la conception du SIS peut inclure plus de redondance dans les équipements, une couverture de diagnostic élargie et des composants plus robustes. A la fin de la conception, un calcul peut alors être exécuté pour déterminer l'intervalle maximal de test permis pour atteindre la caractéristique du SIL définie pour la SIF. Le point négatif dans cette philosophie de conception est que chaque système d'une installation industrielle aura un intervalle de test différent et peut nécessiter un suivi de conformité plus rigoureux. Elle peut également encourager à concevoir les performances orientées vers la partie inférieure de la courbe de performances (par exemple, $PFD_{avg} = 10^{-1}$ pour les systèmes de SIL 1 et $PFD_{avg} = 10^{-2}$ pour des systèmes de SIL 2).

D'autres utilisateurs peuvent souhaiter standardiser sur la base d'un intervalle de test défini et essayer tous les systèmes d'une installation industrielle avec le même intervalle de test. Par exemple, ils peuvent souhaiter essayer chaque SIF annuellement, ainsi ils conçoivent chaque SIS en conséquence. En pré-sélectionnant un intervalle de tests périodiques avant de commencer la conception, les sociétés de l'utilisateur peuvent alors pré-sélectionner des architectures, des composants et la couverture de diagnostic qui satisferont le SIL pour la plupart des applications. En ayant ces caractéristiques déjà définies dans leurs normes internes, elles réduisent les coûts des études de conception, pour la plupart des applications. Dans ce cas, il convient qu'un calcul soit effectué sur le SIS pour s'assurer que les performances de SIL requises seront satisfaites avec l'intervalle de tests périodiques pré-sélectionné.

Dans le choix d'un intervalle de tests périodiques, il convient de considérer le taux de sollicitation, pour les systèmes en mode sollicitation, le taux de défaillance de chaque composant essayé, et les exigences de performances du système global.

NOTE Pour les applications où l'excitation de l'élément de déclenchement final peut ne pas être commode, il convient que la procédure soit écrite de manière à inclure:

a) les essais de l'élément final pendant l'arrêt de l'unité;

b) les essais du SIS en excitant la (les) sortie(s), dans la mesure où cela est possible pendant les essais «en ligne» (par exemple, relais de déclenchement de sortie, solénoïde d'arrêt, ouverture/fermeture partielle d'une vanne);

c) il convient que toute limitation de la période de test des éléments terminaux soit prise en considération dans le calcul de la PFD_{avg} de la SIF.

16.3.1.4 Aucune ligne directrice n'est fournie.

16.3.1.5 Aucune ligne directrice n'est fournie.

16.3.1.6 Aucune ligne directrice n'est fournie.

16.3.2 Inspection

Comme indiqué par la CEI 61511-1, l'inspection du SIS est différente des tests périodiques. Alors qu'un des tests périodiques assure que le SIS fonctionnera correctement, une inspection visuelle est nécessaire pour valider l'intégrité mécanique de l'installation.

Généralement, l'inspection est faite en même temps que le test périodique, mais elle peut être faite plus fréquemment si cela est souhaité.

16.3.1.3 The frequency of proof tests should be consistent with applicable manufacturer's recommendations and good engineering practices, and more frequently, if determined to be necessary by prior operating experience.

There are a number of strategies being used to select the proof test interval for a SIF.

For example, some users like to make this proof test interval as long as possible to minimize maintenance cost and the potential impact of testing. In this case, the SIS design may include more redundancy in equipment, increased diagnostic coverage and robust components. After completion of the design, a calculation may then be performed on the design to determine the maximum test interval allowed to achieve the SIL performance defined for the SIF. The negatives to this design philosophy are that each system in a plant will have a different test interval and may require more rigorous compliance tracking. It also may encourage designing the performance toward the low end of the performance curve (for example, $PFD_{avg} = 10^{-1}$ for SIL 1 systems and $PFD_{avg} = 10^{-2}$ for SIL 2 systems).

Other users may wish to standardize on the basis of a defined test interval and test all systems in a manufacturing plant at the same test interval. For example, they may wish to test each SIF annually so they design each SIS accordingly. By pre-selecting a proof test interval prior to beginning the design, user companies can then pre-select architectures, components and diagnostic coverage that will satisfy the SIL for most applications. By having these features already defined in their corporate standards, it reduces the design engineering cost for most applications. In this case, a calculation should be performed on the SIS to ensure the required SIL performance is satisfied with the pre-selected proof test interval.

In the choice of a proof test interval, considerations should be given to the demand rate for Demand Mode systems, the failure rate of each component being tested, and the overall system performance requirements.

NOTE For those applications where exercising the final trip element may not be practical, the procedure should be written to include:

a) testing the final element during unit shut down;

b) testing the SIS by exercising the output(s) as far as practical (for example, output trip relay, shut down solenoid, partial valve movement) during on-line testing;

c) any limitation of the testing period of the final elements should be taken into account in the calculation of the PFD_{avg} of the SIF.

16.3.1.4 No further guidance provided.

16.3.1.5 No further guidance provided.

16.3.1.6 No further guidance provided.

16.3.2 Inspection

As stated in IEC 61511-1, inspecting the SIS is different from proof testing. Whereas a proof test is ensuring the SIS will operate properly, a visual inspection is required to validate the mechanical integrity of the installation.

Normally, the inspection is done at the same time as the proof test but it may be done at a more frequent interval if desired.

16.3.3 Documentation des essais périodiques et de l'inspection

Il est important de documenter les résultats des tests périodiques et de l'inspection pour consigner/archiver ce qui a été trouvé. Il n'y a pas de prescription spécifique concernant la durée de conservation de ces résultats qu'il convient d'observer, mais généralement une durée suffisante est retenue, de manière à tenir compte du réexamen des résultats précédents, pour voir s'il y a un historique de défaillance de composant.

Par exemple, si un capteur ne réussit pas à passer un test périodique, il est de bonne pratique d'examiner les résultats des tests périodiques précédents, pour voir si ce capteur n'avait pas réussi à passer un test périodique semblable lors des séries d'essais antérieures. Si l'historique indique des défaillances répétées, il convient d'envisager une re-conception du SIS en utilisant un type de capteur différent.

17 Modification du SIS

17.1 Objectifs

Aucune ligne directrice n'est fournie.

17.2 Exigences

17.2.1 Aucune ligne directrice n'est fournie.

17.2.2 Aucune ligne directrice n'est fournie.

17.2.3 Aucune ligne directrice n'est fournie.

17.2.4 Aucune ligne directrice n'est fournie.

17.2.5 Aucune ligne directrice n'est fournie.

17.2.6 Aucune ligne directrice n'est fournie.

18 Déclassement du SIS

18.1 Objectifs

Aucune ligne directrice n'est fournie.

18.2 Exigences

18.2.1 Aucune ligne directrice n'est fournie.

18.2.2 Aucune ligne directrice n'est fournie.

18.2.3 Aucune ligne directrice n'est fournie.

18.2.4 Aucune ligne directrice n'est fournie.

18.2.5 Aucune ligne directrice n'est fournie.

16.3.3 Documentation of proof tests and inspection

It is important to document the results of the proof test and inspection for a record of what was found. There are no specific requirements for how long these results should be retained but generally a sufficient number are retained to allow for re-examination of previous results to see if there is a history of component failure.

For example, if a sensor failed a proof test, it is good practice to review the results of previous proof tests to see if this sensor had failed a similar proof test within the past few tests. If the history indicates repeating failures, consideration should be given to redesigning the SIS using a different type of sensor.

17 SIS modification

17.1 Objective

No further guidance provided.

17.2 Requirements

17.2.1 No further guidance provided.

17.2.2 No further guidance provided.

17.2.3 No further guidance provided.

17.2.4 No further guidance provided.

17.2.5 No further guidance provided.

17.2.6 No further guidance provided.

18 SIS decommissioning

18.1 Objectives

No further guidance provided.

18.2 Requirements

18.2.1 No further guidance provided.

18.2.2 No further guidance provided.

18.2.3 No further guidance provided.

18.2.4 No further guidance provided.

18.2.5 No further guidance provided.

19 Exigences relatives aux informations et à la documentation

19.1 Objectifs

19.1.1 Aucune ligne directrice n'est fournie.

19.2 Exigences

19.2.1 La liste des informations et de la documentation pouvant être utilisée pour mettre en oeuvre un SIS, comprend:

a) les résultats de l'analyse de danger et de risque;
b) les hypothèses utilisées lors de la détermination des niveaux d'intégrité de sécurité;
c) les spécifications des exigences concernant la sécurité;
d) la logique de l'application;
e) la documentation de conception;
f) les informations et/ou la documentation des modifications;
g) les dossiers de vérification et de validation;
h) la (les) procédure(s) de mise en service et de validation du SIS;
i) les procédures opérationnelles du SIS;
j) les procédures de maintenance du SIS;
k) les procédures de tests périodiques;
l) les résultats des évaluations et des audits.

19.2.2 Aucune ligne directrice n'est fournie.

19.2.3 Aucune ligne directrice n'est fournie.

19.2.4 Aucune ligne directrice n'est fournie.

19.2.5 Aucune ligne directrice n'est fournie.

19.2.6 Aucune ligne directrice n'est fournie.

19.2.7 Aucune ligne directrice n'est fournie.

19.2.8 Aucune ligne directrice n'est fournie.

19.2.9 Aucune ligne directrice n'est fournie.

19 Information and documentation requirements

19.1 Objectives

19.1.1 No further guidance provided.

19.2 Requirements

19.2.1 The list of the information and documentation that may be used to implement a SIS, includes:

a) results of the hazard and risk assessment;

b) assumptions used when determining the safety integrity levels;

c) safety requirements specifications;

d) application logic;

e) design documentation;

f) modification information and/or documentation;

g) records of verification and validation;

h) commissioning and SIS validation procedure(s);

i) SIS operating procedures;

j) SIS maintenance procedures;

k) proof test procedures;

l) results of assessments and audits.

19.2.2 No further guidance provided.

19.2.3 No further guidance provided.

19.2.4 No further guidance provided.

19.2.5 No further guidance provided.

19.2.6 No further guidance provided.

19.2.7 No further guidance provided.

19.2.8 No further guidance provided.

19.2.9 No further guidance provided.

Annexe A
(informative)

Techniques données à titre d'exemple pour calculer la probabilité de défaillance sur sollicitation concernant une fonction instrumentée de sécurité

A.1 Généralités

Cette annexe donne en référence un certain nombre de techniques pour calculer les probabilités de défaillance concernant un système instrumenté de sécurité conçu et installé en accord avec la CEI 61511-1. Ces informations sont données à titre d'information et il convient de ne pas les interpréter comme étant les seules techniques d'évaluation qui pourraient être utilisées.

Les méthodologies référencées sont tirées de la CEI 61508-6 – Annexe B, de la CEI 61078, de la CEI 61025, de la CEI 61165 et du rapport technique ISA, TR 84.00.02.

A.2 Technique du schéma fonctionnel de fiabilité

La CEI 61078 et l'Annexe B de la CEI 61508-6 illustrent la technique du schéma fonctionnel de fiabilité pour calculer les probabilités de défaillance, concernant des fonctions instrumentées de sécurité conçues en accord avec la CEI 61511-1 et la présente norme.

A.3 Technique des équations simplifiées

La Partie 2 du rapport TR 84.00.02 de l'ISA illustre une technique d'équation simplifiée pour calculer les probabilités de défaillance concernant des fonctions instrumentées de sécurité conçues en accord avec la CEI 61511-1 et la présente norme.

A.4 Technique d'analyse par arbre de panne

La CEI 61025 et la Partie 3 du rapport TR 84.00.02 de l'ISA illustrent la technique d'analyse par arbre de panne pour calculer les probabilités de défaillance, concernant des fonctions instrumentées de sécurité conçues en accord avec la CEI 61511-1 et la présente norme.

A.5 Technique de modélisation de Markov

La CEI 61165 et la Partie 4 du rapport TR 84.00.02 de l'ISA illustrent la technique de modélisation de Markov pour calculer les probabilités de défaillance, concernant des fonctions instrumentées de sécurité conçues en accord avec la CEI 61511-1 et la présente norme.

Annex A
(informative)

Example of techniques for calculating the probability of failure on demand for a safety instrumented function

A.1 General

This annex references a number of techniques for calculating the probabilities of failure for a safety instrumented system designed and installed in accordance with IEC 61511-1. This information is informative in nature and should not be interpreted as the only evaluation techniques that might be used.

The methodologies referenced are from Annex B of IEC 61508-6, IEC 61078, IEC 61025, IEC 61165, and the ISA TR 84.00.02 series.

A.2 Reliability block diagram technique

IEC 61078 and Annex B of IEC 61508-6 illustrate the reliability block diagram technique for calculating the probabilities of failure for safety instrumented functions designed in accordance with IEC 61511-1 and this standard.

A.3 Simplified equations technique

ISA TR 84.00.02-2 illustrates a simplified equation technique for calculating the probabilities of failure for safety instrumented functions designed in accordance with IEC 61511-1 and this standard.

A.4 Fault tree analysis technique

IEC 61025 and ISA TR 84.00.02-3 illustrate the fault tree analysis technique for calculating the probabilities of failure for safety instrumented functions designed in accordance with IEC 61511-1 and this standard.

A.5 Markov modelling technique

IEC 61165 and ISA TR 84.00.02-4 illustrate the Markov modelling technique for calculating the probabilities of failures for safety instrumented functions designed in accordance with IEC 61511-1 and this standard.

Annexe B
(informative)

Développement typique d'une architecture de SIS

B.1 Informations de base

B.1.1 Introduction

Ce qui suit est donné comme exemple pour illustrer les diverses étapes à accomplir pour développer une architecture de SIS satisfaisant aux exigences de la CEI 61511-1. L'ingénierie du SIS suit des directives, des règles, et utilise des équipements normalisés comme décrit ci-dessous.

B.1.2 Directives et règles

Dans le passé, les applications de sécurité se sont appelées «Systèmes d'instrument critiques». Des règles d'ingénierie, des exemples typiques et de meilleures pratiques, ainsi que des procédures d'essai ont été développés.

Il existe des directives pour déterminer la fonction instrumentée de sécurité (SIF) et le SIL requis, avec l'analyse de couche de protection (LOPA, comme l'Annexe «F» de la CEI 61511-3), ainsi que la redondance d'instruments et les pratiques en matière de conception.

B.1.3 Instrumentation

L'instrumentation dans les applications de sécurité (SIS) utilise les informations du fournisseur concernant les diagnostics et la proportion de défaillances en sécurité (SFF), ainsi que les informations de performances collectées à partir des applications, pour calculer la probabilité de la défaillance sur sollicitation (PFD).

B.1.4 Unité logique

Le matériel, le logiciel système et le système de développement de l'unité logique sont conformes au SIL 3 de la CEI 61508 et ont un langage de variabilité limitée pour le programme d'application.

Le manuel de sécurité du système donne des directives détaillées sur l'application du système et sur le développement du logiciel d'application.

Les fonctions de sécurité standards définissables par l'utilisateur (par exemple, détection d'anomalie du transmetteur, choix de la redondance, telle que 1oo2, 2oo3, et priorité de sécurité de sortie) sont disponibles en tant que modèles de programme d'application. Les modèles sont développés par l'utilisateur.

B.2 Processus de travail

B.2.1 Introduction

Toutes les activités d'ingénierie suivent un processus de travail, pour le projet global, prédéfini. Le développement d'un SIS a son propre processus. Différentes étapes sont tracées dans le processus global. L'évaluation fonctionnelle de sécurité est effectuée aux étapes appropriées.

Annex B
(informative)

Typical SIS architecture development

B.1 Background

B.1.1 Introduction

The following is provided as an example to illustrate the various steps performed to develop a SIS architecture, which satisfies the requirements of IEC 61511-1. SIS engineering follows guidelines and practices and uses standardized equipment as outlined below.

B.1.2 Guidelines and practices

In the past, safety applications were called "critical instrument systems". Engineering rules, typical examples and best practices as well as test procedures were developed.

Guidelines to determine the required safety instrumented function and SIL with Layer of Protection Analysis (LOPA, as in Annex F of IEC 61511-3), as well as instrument redundancy and design practices exist.

B.1.3 Instrumentation

Instrumentation in safety applications (SIS) utilises vendor information on diagnostics and safe failure fraction (SFF) as well as performance information collected from the applications to calculate the probability of failure on demand (PFD).

B.1.4 Logic solver

The hardware, system software and development system of the logic solver is IEC 61508 SIL 3 compliant and has a limited variability language for its application program.

The system Safety Manual gives detailed guidance on the system application and application software development.

Standard user definable safety functions (for example, transmitter fault detection, redundancy selection such as 1oo2, 2oo3, and output safety override) are available as application program templates. Templates are user developed.

B.2 Work process

B.2.1 Introduction

All engineering activities follow a predefined overall project work process. The development of a SIS has its own process. Individual steps are mapped into the overall process. Functional safety assessment is carried out at the appropriate stages.

B.2.2 Etapes typiques du cycle de vie du SIS

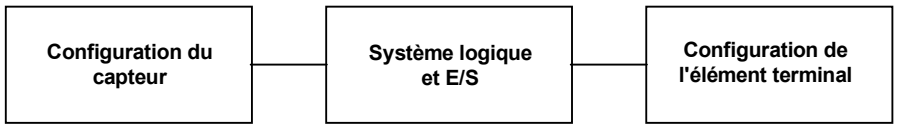
Développer une application de SIS nécessite les étapes typiques suivantes. Dans la suite, nous traiterons seulement des étapes 3, 4 et des parties de l'étape 5 relatives à l'architecture du système.

Etape	Titre	Activité
1.	Domaine d'application	Définir les équipements du processus
2.	Exigences fonctionnelles de sécurité des équipements du processus	Définir le potentiel de danger, Exécuter l'analyse du niveau de protection (LOPA)
3.	Affectation des exigences de sécurité du système	Conception de la structure du SIS
4.	Affectation des exigences de sécurité au sein du SIS	Identifier le matériel du SIS
5.	Développement du logiciel d'application	Conception du logiciel du SIS
6.	Essais et validation du logiciel d'application	Essais du SIS
7.	Installation	Installation sur le terrain
8.	Mise en service	Recette globale
9.	Exploitation	Exécution du processus

B.2.3 Affectation des exigences de sécurité

Informations disponibles à partir de LOPA: Spécification des exigences concernant la sécurité et le SIL pour l'application du SIS (par exemple, SIL pour chaque SIF).

Modèle utilisé pour réaliser le SIL.



IEC 1830/03

Détermination de la PFD: la PFD globale (voir ci-dessus) reste dans les limites du SIL.

Méthode abrégée: des configurations d'instrumentation standards comprenant des types redondants (par exemple, 1oo2), des diagnostics disponibles et des intervalles d'essai, peuvent être fournies dans des tables en rapport avec les exigences de SIL. Il convient que ces tables soient basées sur des données expérimentales et sur une conception validée de diverses applications de processus au sein de l'installation. La combinaison de configurations alternatives de systèmes avec des éléments de données connues, et avec des schémas fonctionnels, permet la sélection du choix le plus approprié.

Spécification des composants du SIS: tous les composants du système ont des caractéristiques validées (par exemple, PFD, SFF, tolérance aux anomalies, exigences systématiques pour le SIL spécifié), comme cela est demandé dans la CEI 61511-1.

– **Les capteurs et les éléments terminaux** sont convenablement choisis en fonction de l'application du processus et les diverses caractéristiques types sont normalisés par le département/service d'ingénierie en fonction de l'expérience opérationnelle.

– **Les systèmes logiques** – L'E/S est spécifiée en fonction des exigences du capteur et de l'élément terminal. L'unité logique, le langage d'application, les outils de développement et l'interface de communication font partie du système de sécurité approuvé. L'interface opérateur peut être personnalisée en fonction des exigences de l'application.

B.2.2 Typical SIS lifecycle steps

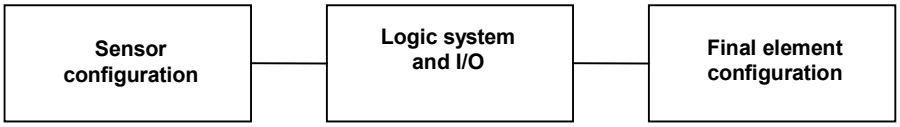
Developing a SIS application requires the following typical steps. In the following we will only discuss step 3, 4 and those parts of step 5 which are related to the system architecture.

Step	Title	Activity
1	Application scope	Define process equipment
2	Functional safety requirements of the process equipment	Define hazard potential , perform Level Of Protection Analysis (LOPA)
3	System safety requirement assignment	Design SIS structure
4	Safety requirement assignment within the SIS	Identify SIS hardware
5	Application software development	Design SIS software
6	Application software testing and validation	Test SIS
7	Installation	Field installation
8	Commissioning	Overall acceptance
9	Operation	Run process

B.2.3 Safety requirement assignment

Available information from LOPA: safety requirements specification and SIL for the SIS application (for example, SIL for each SIF).

Model used to achieve SIL:



IEC 1830/03

Determination PFD: the overall PFD (see above) stays within the SIL limits.

Abridged method: standard instrumentation configurations including redundancy types (for example,1oo2), available diagnostics and test intervals can be provided in Tables related to the SIL requirements. These Tables should be based on experience data and proven design of various process applications within the facility. Combining alternative system configurations with known element data to block diagrams enables the selection of the most appropriate choice.

SIS component specification: all system components have proven characteristics (for example, PFD, SFF, fault tolerance, systematic requirements for the specified SIL) as mandated in IEC 61511-1.

- **sensors and final elements** are appropriately selected for the process application and various type features are standardized by the engineering department according to operating experience.
- **logic systems:** I/O is specified according to sensor and final element requirements. The logic solver, application language, development tools and communication interface is part of the approved safety system. The operator interface can be tailored to application requirements.

B.2.4 Affectation des exigences de sécurité au sein du SIS

Dans cette étape, toutes les fonctions de la spécification des exigences concernant la sécurité sont affectées aux composants, aux fonctions ou au logiciel du système. Les exigences d'intégrité de sécurité détermineront les composants appropriés du SIS et l'architecture possible du SIS.

B.2.5 Exigences relatives à l'architecture du logiciel d'application

Après le choix de l'architecture du SIS, le logiciel d'application peut devoir être spécifié pour l'implémentation de la redondance (par exemple, 1oo2) et/ou des diagnostics, comme cela est demandé pour les capteurs, l'unité logique et les éléments terminaux.

B.2.6 Développement du logiciel d'application

Le langage de programmation est un langage en blocs fonctionnels (un langage de variabilité limitée). Le développement du code et les essais sont des processus bien connus. De plus, plusieurs restrictions concernant la programmation des fonctions de sécurité sont décrites en détails dans le manuel de sécurité du système.

B.3 Exemple 1

B.3.1 Introduction

L'exemple utilisé ci-dessous n'est pas issu d'un véritable scénario, et il passe sous silence la considération des défaillances de cause commune avec d'autres couches de sécurité. Il est spécialement construit pour démontrer comment appliquer le processus de conception du SIS décrit précédemment.

B.3.2 Scénario dangereux

La commande de la température d'un réacteur chauffé par la vapeur est défaillante et ouvre entièrement la vanne de commande de vapeur.

B.3.3 SRS et SIL

Spécification des exigences concernant la sécurité: Si la pression du réacteur excède 10 bars, fermer/isoler l'arrivée de vapeur dans la chemise de ce dernier, dans les 20 secondes, pour éviter une réaction exothermique. Aucune action d'un opérateur n'est nécessaire. Le SIL requis est de 3.

B.3.4 Architecture du système

Composants du système: configuration du capteur de pression, configuration de l'unité logique, configuration de l'élément terminal. Les capteurs intelligents validés en utilisation sont directement connectés aux entrées du système logique. La vanne de sectionnement d'urgence a une électrovanne intégrée et est directement connectée aux sorties du système logique. Toutes les données de MTTF sont issues de résultats en exploitation réelle.

Instrumentation disponible:

– Les capteurs de pression sont conformes au 11.4.4 de la CEI 61511-1: MTTF 10^5 h, DC= 70 %, SFF = 90 %, intervalle des tests périodiques: un an, MTTR = 8 h.

– La vanne de sectionnement d'urgence est conforme au 11.4.4 de la CEI 61511-1: MTTF 8 $\times$ 10^4 h, DC = 0 %, SFF = 60 %, intervalle des tests périodiques: 6 mois, MTTR = 8 h.

B.2.4 Safety requirement assignment within the SIS

In this step, all functions of the safety requirements specification are allocated to system components, functions or software. Safety integrity requirements will determine the appropriate SIS components and the possible SIS architecture.

B.2.5 Architecture related application software requirements

After selection of the SIS architecture, application software may have to be specified for implementation of redundancy (for example, 1oo2) and/or diagnostics, as required for sensors, logic solver, and final elements.

B.2.6 Application software development

The programming language is function block diagram (a limited variability language). Code development and testing is a well known process. Additionally, there are several restrictions for safety function programming which are described in the system Safety Manual in detail.

B.3 Example 1

B.3.1 Introduction

The example used below is not from a real scenario, and excludes consideration of common cause failures with other safety layers. It is specially composed to demonstrate how to apply the previous described SIS design process.

B.3.2 Hazardous scenario

Temperature control of a steam heated reactor fails and opens the steam control valve fully.

B.3.3 SRS and SIL

Safety requirements specification: if reactor pressure exceeds 10 bar, close off steam to the reactor jacket within 20 seconds to avoid exothermic reaction. There is no operator action necessary. The required SIL is 3.

B.3.4 System architecture

System components: pressure sensor configuration, logic solver configuration, final element configuration. Proven in use smart sensors are directly connected to inputs of the logic system. Emergency block valve has solenoid valve integrated and is directly connected to outputs of the logic system. All MTTF data come from actual operating experience.

Available instrumentation:

- pressure sensors comply with 11.4.4 of IEC 61511-1: MTTF 10^5 h, DC = 70 %, SFF = 90 %, proof test interval every year, MTTR = 8 h.
- emergency block valve complies with 11.4.4 of IEC 61511-1: MTTF 8×10^4 h, DC = 0 %, SFF = 60 %, proof test every 6 months, MTTR = 8 h.

PFD relative à un élément unique:

– Capteur: $2{,}2 \times 10^{-3}$ (voir Article A.1) – non acceptable

– Unité logique (redondante): $1{,}3 \times 10^{-4}$ comprenant l'interface d'E/S (à partir de certificat/justification)

– Vanne: $2{,}41 \times 10^{-3}$ (voir Article A.1) – non acceptable

Recherche de l'architecture de capteurs acceptable: choisissez la redondance 1oo2, cause commune = 10 %, DC = 90 % (voir Article A.1)
nouvelle PFD pour l'architecture de capteurs 1oo2: 2.3×10^{-4}
Vérifier Tableau 6 et 11.4.4 de la CEI 61511-1, tolérance aux anomalies réelles = 1 → SIL 3 - - acceptable

Recherche de l'architecture des éléments terminaux acceptable: choisissez la redondance 1oo2,
cause commune = 10 %, (voir Article A.1)
nouvelle PFD pour l'architecture des éléments terminaux 1oo2: $4{,}65 \times 10^{-4}$
Vérifier Tableau 6 et 11.4.4 de la CEI 61511-1, tolérance aux anomalies réelles = 1 → SIL 3 - - acceptable

Vérification de la PFD: capteur + unité logique + élément terminal
$(2{,}3 + 1{,}3 + 4{,}7) \times 10^{-4} = 8{,}3 \times 10^{-4} < 10^{-3}$

B.3.5 Logiciel de sécurité relatif à l'architecture supplémentaire

Logiciel de configuration du capteur: Pour le choix ci-dessus du signal du capteur 1oo2, le logiciel est programmé (bloc fonctionnel existant) pour fermer la vanne de vapeur si:

- l'un des deux capteurs lit une condition dépassant la valeur de processus spécifiée;
- le diagnostic révèle une défaillance dangereuse.

Logiciel de configuration d'élément terminal: Les deux sorties de vanne de vapeur sont désactivées dans le cas où une action de sortie sûre est commandée par le programme de sécurité.

B.4 Exemple 2

B.4.1 Introduction

Exemple semblable avec des conséquences ayant pour résultat un SIL inférieur.

B.4.2 Scénario dangereux

La commande de la température d'un réacteur chauffé par la vapeur est défaillante et ouvre entièrement la vanne de commande de vapeur.

B.4.3 SRS et SIL

Spécification des exigences concernant la sécurité: si la pression du réacteur à fonctionnement discontinu excède 10 bars, fermer/isoler l'alimentation du réactif «A» vers le réacteur, dans les 20 secondes, pour éviter une réaction exothermique. Aucune action d'un opérateur n'est nécessaire. Le SIL requis est de 2.

B.4.4 Architecture du système

Composants du système: configuration du capteur de pression, configuration de l'unité logique, configuration de l'élément terminal. Les capteurs intelligents validés en utilisation sont directement connectés aux entrées du système logique. La vanne de sectionnement d'urgence a une électrovanne intégrée et est directement connectée aux sorties du système logique. Toutes les données de MTTF sont issues de résultats en exploitation réelle.

Single element PFD:

- sensor: $2{,}2 \times 10^{-3}$ (see Clause A.1) – not acceptable.
- logic solver (redundant): $1{,}3 \times 10^{-4}$ including I/O interface (from certificate).
- valve: $2{,}41 \times 10^{-3}$ (see Clause A.1) – not acceptable.

Find acceptable sensor architecture: select 1oo2 redundancy.
Common cause = 10 %, DC = 90 % (see Clause A.1).
New PFD for 1oo2 sensor architecture: $2{,}3 \times 10^{-4}$.
Check Table 6 of IEC 61511-1 and 11.4.4 of IEC 61511-1, actual fault tolerance = 1 → SIL 3 – acceptable.

Find acceptable final element architecture: select 1oo2 redundancy.
Common cause = 10 %, (see Clause A.1).
New PFD for 1oo2 final element architecture: $4{,}65 \times 10^{-4}$.
Check Table 6 and 11.4.4 of IEC 61511-1, actual fault tolerance = 1 → SIL 3 – acceptable.

PFD check: sensor + logic solver + final element.
$(2{,}3 + 1{,}3 + 4{,}7) \times 10^{-4} = 8{,}3 \times 10^{-4} < 10^{-3}$

B.3.5 Additional architecture related safety software

Sensor configuration software: for the above 1oo2 sensor signal selection software is programmed (existing function block) to close the steam valve if:

- one of the two sensors reads a condition exceeding the specified process value;
- the diagnostic reveals a dangerous failure.

Final element configuration software: both steam valve outputs are de-energized in the case that a safe output action is commanded by the safety program.

B.4 Example 2

B.4.1 Introduction

Similar example with consequences resulting in a lower SIL.

B.4.2 Hazardous scenario

Temperature control of a steam heated reactor fails and opens the steam control valve fully.

B.4.3 SRS and SIL

Safety requirements specification: if batch reactor pressure exceeds 10 bar, close off feed of reactant “A” to the reactor within 20 seconds to avoid exothermic reaction. There is no operator action necessary. The required SIL is 2.

B.4.4 System architecture

System components: pressure sensor configuration, logic solver configuration, final element configuration. Proven in use smart sensors are directly connected to inputs of the logic system. Emergency block valve has solenoid valve integrated and is directly connected to outputs of the logic system. All MTTF data are actual operating experience.

Instrumentation disponible:

– Les capteurs de pression sont conformes au 11.4.4 de la CEI 61511-1: MTTF 10^5 h, DC= 70 %, SFF = 90 %, intervalle des tests périodiques: un an, MTTR = 8 h.

– La vanne de sectionnement d'urgence est conforme au 11.4.4 de la CEI 61511-1: MTTF $2{,}5 \times 10^4$ h, DC = 0 %, SFF = 60 %, intervalle des tests périodiques: une semaine (168 h), MTTR = 8 h.

PFD relative à un élément unique:

– Capteur: $2{,}2 \times 10^{-3}$ (voir Article A.1) – acceptable

– Unité logique (redondante): $1{,}3 \times 10^{-4}$ comprenant l'interface d'E/S (à partir de certificat/justification)

– Vanne: voir ci-dessous (formule: voir Article A.1)

PFD relative à un capteur unique:

PFD pour l'architecture de capteur 1oo1: $2{,}2 \times 10^{-3}$
Vérifier le Tableau 6 et le paragraphe 11.4.4 de la CEI 61511-1, tolérance aux anomalies réelles = 0 $\rightarrow$ SIL 2 -- acceptable

PFD relative à un élément terminal unique: (formule voir l'Annexe A, Article A1 de la CEI 61511-2)
PFD = $\lambda_D \times t_{CE}$, $\lambda_D = 1/(25\,000 \times 2)$, $t_{CE} = 168/2 + 8$
PFD pour l'architecture de l'élément terminal 1oo1: $1{,}84 \times 10^{-3}$
Vérifier le Tableau 6 et 11.4.4 de la CEI 61511-1, tolérance aux anomalies réelles = 0 $\rightarrow$ SIL 2 -- acceptable

Vérification de la PFD: capteur + unité logique + élément terminal
$(2{,}2 + 0{,}1 + 1{,}8) \times 10^{-3} = 4{,}1 \times 10^{-3} < 10^{-2}$

B.4.5 Logiciel de sécurité relatif à l'architecture supplémentaire

Logiciel de configuration d'élément terminal: La sortie de vanne de vapeur est désactivée lorsqu'une action de sortie sûre est commandée par le programme de sécurité.

De plus, le logiciel de surveillance est écrit de telle sorte qu'il montre que l'état de sécurité de la vanne est atteint chaque fois que la vanne est actionnée (une fois par lot, typiquement toutes les 8 h). En cas de défaillance de l'essai ou si plus de 168 h se sont écoulées depuis le dernier essai, la sortie de l'unité logique reste dans l'état de sécurité (vanne de sectionnement d'urgence fermée) et l'état d'alarme est activé. Cet essai automatique permet de paramétrer l'intervalle de tests périodiques, dans le calcul de la PFD, à 168 h.

Available instrumentation:

- Pressure sensors comply with 11.4.4 of IEC 61511-1: MTTF 10^5 h, DC = 70 %, SFF = 90 %, proof test interval every year, MTTR = 8 h.
- Emergency block valve complies with 11.4.4 of IEC 61511-1: MTTF $2,5 \times 10^4$ h, DC = 0 %, SFF = 60 %, proof test every week (168 h), MTTR = 8 h.

Single element PFD:

- Sensor: $2,2 \times 10^{-3}$ (see Clause A.1) – acceptable.
- Logic solver (redundant): $1,3 \times 10^{-4}$ including I/O interface (from certificate).
- Valve: see below (see Clause A.1 for the formula).

Single sensor PFD:

PFD for 1oo1 sensor architecture: $2,2 \times 10^{-3}$.
Check Table 6 and 11.4.4 of IEC 61511-1, actual fault tolerance = 0 → SIL 2 – acceptable.

Single final element PFD: (see Clause A.1 for the formula).
PFD = $\lambda_D \times t_{CE}$, λ_D = 1/(25 000 x 2), t_{CE} = 168/2 + 8
PFD for 1oo1 final element architecture: $1,84 \times 10^{-3}$.
Check IEC 61511-1 Table 6 and 11.4.4, actual fault tolerance = 0 → SIL 2 - acceptable.

PFD check: sensor + logic solver + final element.
$(2,2 + 0,1 + 1,8) \times 10^{-3} = 4,1 \times 10^{-3} < 10^{-2}$

B.4.5 Additional architecture related safety software

Final element configuration software: The steam valve output is de-energized when a safe output action is commanded by the safety program**.**

Additionally, monitoring software which proves that the safe state of the valve is reached each time the valve is operated (once per batch, typically every 8 hours) is written. In case of a test failure or if more than 168 hours have elapsed since the last test, the logic solver output stays in the safe state (emergency block valve closed) and the condition is alarmed. This automatic test allows setting the proof test interval in the PFD calculation to 168 hours.

Annexe C
(informative)

Fonctions applicatives d'un AP de sécurité

Ce qui suit est un survol de quelques étapes clé, qu'un intégrateur considère, lorsqu'il utilise un petit automate programmable (AP) de sécurité (par exemple, moins de 150 E/S) dans une application de SIS. Il est présenté pour aider le lecteur pendant la planification initiale de la conception.

L'AP de sécurité est une unité logique de SIS certifiée suivant la CEI 61508. Pour une application de sécurité spécifique, les capteurs et les éléments terminaux sont connectés aux bornes d'E/S de l'unité logique du SIS et le programme d'application est mis en oeuvre. Toutes les fonctionnalités de sécurité se rapportant à des défaillances de l'unité logique du SIS (par exemple, vérifications «en ligne», contrôles de temps) font partie du système intégré. Les contrôles des capteurs et des éléments terminaux nécessaires sont mis en oeuvre dans le logiciel d'application; pour certaines fonctions, il existe des blocs fonctionnels approuvés.

Les données d'intégrité de sécurité (par exemple, PFD, limite de revendication de SIL, etc.) de tous les dispositifs existent. Les données d'intégrité de sécurité de l'unité logique sont données par le manuel de cette dernière.

C.1 Système

L'unité logique du SIS est un AP, qui est spécifiquement conçu pour des applications de sécurité. C'est un type approuvé pour satisfaire à la CEI 61508 jusqu'à un SIL 3. Il a des interfaces d'entrée et de sortie pour les signaux du processus relatifs à la sécurité et pour les communications avec d'autres AP de sécurité. Il a également des interfaces pour les signaux et les communications qui ne sont pas sécuritaires. Le système se compose de:

– une unité centrale de traitement (CPU) avec des caractéristiques de matériel spéciales pour la sécurité fonctionnelle, un système d'exploitation spécial et des fonctions intégrées pour le contrôle des défaillances (pour la programmation de l'application et l'intégration du logiciel, la redondance intégrée est couverte par le système de développement; le programmeur ne voit qu'une unité centrale de traitement);
– du système de développement pour le langage de variabilité limitée (par exemple, langage en blocs fonctionnels);
– la bibliothèque avec des blocs fonctionnels approuvés;
– un outil spécial de configuration pour les paramètres de fonction instrumentée de sécurité;
– un outil pour confirmer que le moteur d'exécution de l'application téléchargé est identique au logiciel d'application source;
– un manuel de sécurité.

Annex C
(informative)

Application features of a safety PLC

The following is an outline of some key steps an integrator considers when utilizing a small (for example, less than 150 I/O) safety PLC in a SIS application. It is presented to assist the reader during initial design planning.

The safety PLC is a certified SIS logic solver per the IEC 61508 series. For a specific safety application, sensors and final elements are connected to the SIS logic solver I/O terminals and the application program is implemented. All safety functionalities referring to failures of the SIS logic solver (for example, online checks, time control) are part of the embedded system. Necessary checks of sensors and final elements are implemented within the application software; for some functions, approved function blocks exist.

Safety integrity data (for example, PFD, SIL claim limit, etc) of all devices exist. Safety integrity data of the logic solver is given in the manual of the logic solver.

C.1 System

The SIS logic solver is a PLC, which is specifically designed for safety applications. It is type approved to comply with the IEC 61508 series up to SIL 3. It has input and output interfaces for safety-related process signals and communication with other safety PLC's. It also has interfaces for signals and communication which are not safety-related. The system consists of:

- CPU with special hardware features for functional safety, a special operating system and embedded functions for control of failures (for application programming and software integration the integrated redundancy is covered by the development system. The programmer sees only one CPU);
- development system for limited variability language (for example, function block diagram);
- library with approved function blocks;
- special configuration tool for safety instrumented function parameters;
- tool to confirm that the downloaded run-time application software is identical to the source application software;
- Safety Manual.

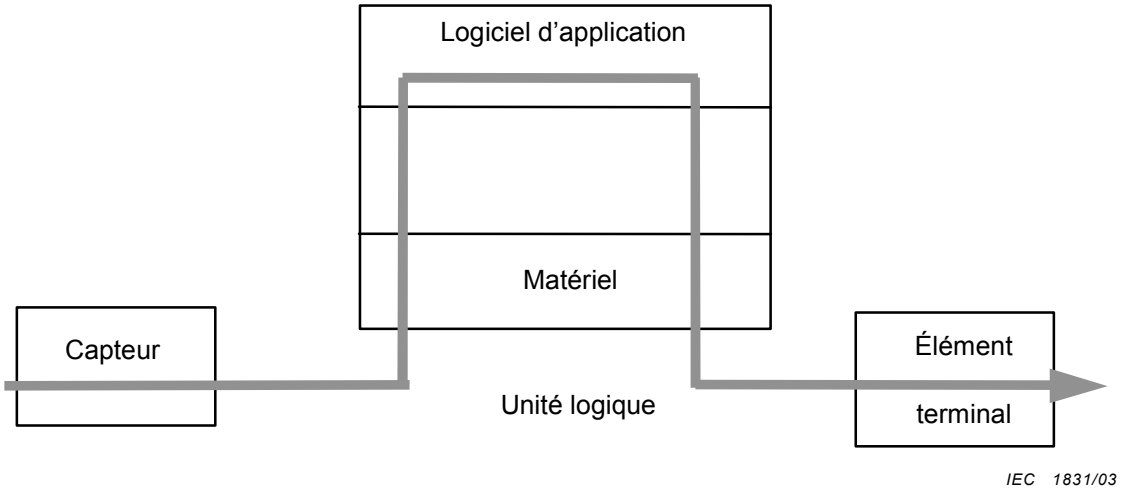


Figure C.1 – Unité logique

C.2 Processus de travail

a) La spécification des exigences concernant la sécurité sera conforme à cette norme: quelques considérations importantes sont données ci-dessous:

   1) la spécification de toutes les fonctions instrumentées de sécurité;
   2) la plage des entrées analogiques;
   3) la définition des diagnostics «en ligne» des capteurs et des éléments terminaux;
   4) la description des réactions du système en cas de modes de défaillances détectées;
   5) la définition des paramètres des fonctions instrumentées de sécurité (par exemple, temps maximal de cycle, temps alloué maximal de divergence des entrées comparées);
   6) des restrictions dans le manuel de sécurité.

b) Il convient que la spécification des exigences concernant la sécurité du logiciel d'application soit dérivée de 1).

   Les exigences concernant la sécurité se rapportant au matériel de l'unité logique (AP) sont décrites dans le manuel de sécurité. Les contraintes se réfèrent principalement à des points tels que les limites de performances, la taille mémoire, le temps de réponse.

   Les contraintes pour l'architecture du logiciel et l'implémentation du code sont décrites dans le manuel de sécurité. Elles se réfèrent au système de développement de l'AP. La plupart des contraintes sont implicitement données par le langage de variabilité limitée.

c) Conception architecturale du logiciel d'application

   Il convient que la conception architecturale de l'application reflète étroitement les fonctions instrumentées de sécurité et les modes d'exploitation spécifiés pour le processus.

d) Développement du logiciel d'application

   Le développement du logiciel d'application est facilité par l'utilisation des blocs fonctionnels existants.

e) Intégration

   L'intégration implique le téléchargement des données de configuration (par exemple, tables d'E/S) et du logiciel d'application et le réglage de tous les paramètres, qui sont différents des réglages par défaut.

f) Vérification

   Le logiciel d'application est vérifié avant l'intégration du système ou après l'intégration du système. La vérification est supportée par l'environnement de développement.

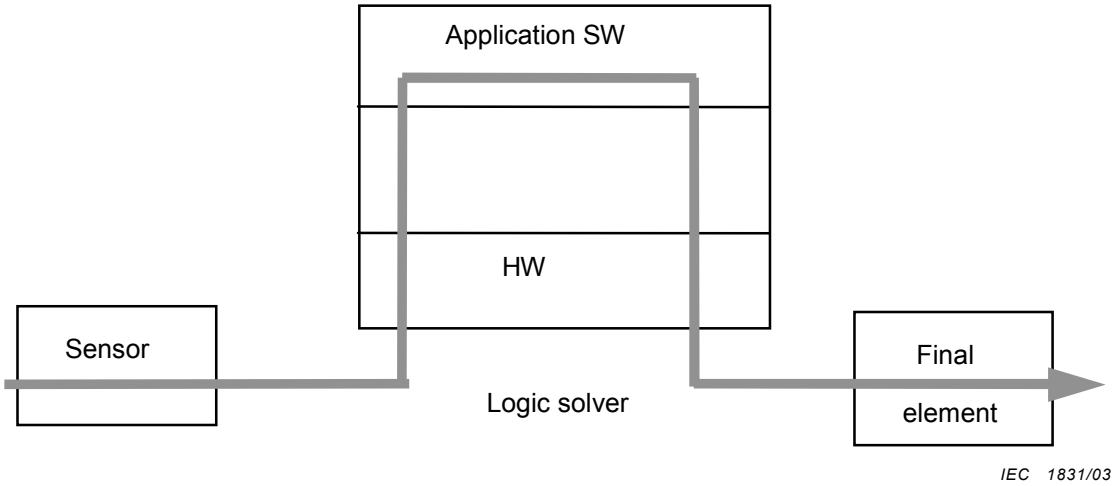


Figure C.1 – Logic solver

C.2 Work process

a) Safety requirements specification will conform to this standard: the following are some key considerations:

   1) specification of all safety instrumented functions;
   2) the range of analogue inputs;
   3) definition of online diagnostics of sensors and final elements;
   4) description of system reactions in case of detected failure modes;
   5) definition of safety instrumented function parameters (for example, maximum cycle time, maximum allowed time of discrepancy of compared inputs);
   6) restrictions in the Safety Manual.

b) Application software safety requirements specification should be derived from a).

   Safety requirements referring to the logic solver hardware (PLC) are described in the Safety Manual. The constraints refer mainly to such items as performance limits, memory size, response time.

   Constraints for software architecture and code implementation are described in the Safety Manual. They refer to the development system of the PLC. Most of the constraints are implicitly given by limited variability language.

c) **Application software architectural design:** the application architectural design should closely reflect the safety instrumented functions and modes of operation specified for the process.

d) **Application software development:** application software development is facilitated by the use of existing function blocks.

e) **Integration:** integration involves the downloading of the configuration data (for example, I/O Tables) and application software and the setting of all parameters, which are different from the default settings.

f) **Verification:** application software is verified before system integration or after system integration. Verification is supported by the development environment.

Annexe D
(informative)

Exemple de méthodologie de développement du logiciel d'application d'une unité logique de SIS

Cet exemple illustre comment un intégrateur d'une unité logique de SIS particulière développe le logiciel d'application de sécurité pour ses clients. Ce logiciel est typiquement développé en tant que partie d'un procédé d'intégration du système global, qui est commenté ci-dessous.

Puisque l'accent est mis sur la méthodologie de développement du logiciel d'application de sécurité, il est important de discuter des outils de développement du logiciel d'application, des langages de programmation et des normes de codage, qui ont été utilisés pour développer les programmes d'application. Le but de cette discussion est de fournir un exemple de caractéristiques typiques des outils de développement du logiciel, des langages de programmation et des traducteurs de langage associés, qui sont fournis dans une logique de SIS.

L'unité logique de SIS a des outils de développement de programmation du logiciel d'application qui supportent un certain nombre de langages indiqués dans la CEI 61131-3. La CEI 61131-3 définit un certain nombre de langages pour la programmation générale des automates programmables. Etant donné que la CEI 61311-3 ne traite pas des applications de sécurité, il a été décidé

– d'utiliser les langages de variabilité limitée communs au domaine des processus;
– d'éliminer les concepts/constructions de langage qui ne sont pas appropriées pour des applications de sécurité;
– d'utiliser une norme de codage pour restreindre davantage l'emploi de concepts/ constructions de langage pour des applications critiques;
– d'incorporer des dispositifs/fonctions de sécurité d'accès et de protection de fichier;
– d'approvisionner des bibliothèques certifiées des fonctions de la CEI 61131-3, des blocs fonctionnels et des fonctions relatives au processus (par exemple, traitement de données analogiques, capteurs d'incendie et de gaz);
– de pourvoir à la certification par une tierce partie des outils de développement du logiciel de programmation de l'application, des bibliothèques et des traducteurs de langage.

Ces décisions sont commentées plus en détails à l'Article D.2, qui concerne le logiciel de développement de l'application.

Un exemple de norme de codage utilisée par les programmeurs de l'unité logique du SIS est également commenté à l'Article D.3. L'Article D.4 traite des exigences supplémentaires qu'il convient de considérer pour les outils de développement du logiciel.

D.1 Résumé du procédé d'intégration du système global

Les principaux services d'intégration de système instrumenté de sécurité fournis avec l'unité logique du SIS consistent en un certain nombre d'activités comprenant les éléments décrits par les points a) à g) ci-dessous.

Annex D
(informative)

Example of SIS logic solver application software development methodology

This example illustrates how one particular SIS logic solver integrator develops safety application software for its customers. This software is typically developed as a part of an overall system integration process that is discussed in the section below.

Since the emphasis is on the safety application software development methodology, it is important to discuss the application software development tools, programming languages and coding standards that were used to develop the application programs. The purpose of this discussion is to provide an example of the typical features of the software development tools, the programming languages and associated language translators that are provided in a SIS logic.

The SIS logic solver has application programming software development tools that support a number of IEC 61131-3 languages. The IEC 61131-3 standard defines a number of languages for the general purpose programming of Programmable Logic Controllers. Since the IEC 61311-3 standard does not address safety applications, it was decided to:

- use limited variability languages common to the process sector;
- eliminate language constructs that are not appropriate for safety applications;
- use a coding standard to further restrict the use of language constructs for critical applications;
- incorporate access security and file protection features;
- supply certified libraries of IEC 61131-3 functions, function blocks, and process related functions (for example, analogue data processing, fire and gas sensors);
- provide third-party certification of the application programming software development tools, libraries, and language translators.

These decisions are discussed in more detail in Clause D.2 on application development software.

An example of a coding standard used by the SIS logic solver programmers is also discussed in Clause D.3. Clause D.4 discusses additional requirements that should be considered for the software development tools.

D.1 Summary of the overall system integration process

The major safety instrumented system integration services provided with the SIS logic solver consisted of a number of activities including.

a) L'intégration du matériel

Ceci comprend l'installation de l'unité logique du SIS dans des coffrets, avec les panneaux de raccordements appropriés pour connecter les signaux du processus aux modules d'E/S de l'unité logique. Les alimentations en énergie et la distribution d'énergie pour l'unité logique et les dispositifs de terrain sont en principe également incluses.

b) Définition de la logique de l'application

Les services d'intégration de l'unité logique du SIS peuvent également définir la logique détaillée, en travaillant étroitement avec les ingénieurs du client. La logique de l'application, pour chaque fonction instrumentée de sécurité, est définie en tenant compte de la redondance du capteur et de d'élément terminal. L'interface relative aux essais et à la maintenance du SIS pendant que le processus est en cours d'exécution est également définie, pour remplir les exigences opérationnelles du client. La logique critique non sécuritaire supplémentaire peut également être incluse, mais est strictement séparée, et elle est conçue suivant la même norme que la fonction de sécurité.

c) Implémentation du logiciel d'application et configuration du matériel

Le progiciel de développement du logiciel d'application, certifié du point de vue sécurité, de l'unité logique du SIS est utilisé pour configurer les E/S de l'unité logique du SIS et le matériel de communication. Les logiciels d'application, pour chaque fonction instrumentée de sécurité, ainsi que les logiciels d'application non critique, sont également implémentés et essayés.

d) Essais de recette en usine

De nombreux clients effectuent un essai de recette en usine, pour vérifier le fonctionnement correct du matériel et du logiciel d'application, avant qu'ils ne soient livrés sur le site de l'installation industrielle. Le matériel et le logiciel d'application sont entièrement essayés par les ingénieurs du client et par d'autres personnes exploitantes.

e) Installation du SIS sur le site du client

Soit l'installation, soit la supervision de l'installation par le fournisseur est faite sur le site de l'installation industrielle.

f) Essais de recette sur site

Chaque capteur et chaque interface d'élément terminal dans les unités logiques du SIS est vérifié pour s'assurer de son bon fonctionnement et de son étalonnage correct. Les entités comme le logiciel d'application global, les fonctions de dérivation pour la maintenance, sont de nouveau essayés.

g) Modifications du logiciel d'application et du matériel

Après l'installation et les opérations initiales, les modifications au logiciel d'application et au matériel sont mises en œuvre, en utilisant les strictes procédures de modification approuvées pour l'installation industrielle.

D.2 Logiciel de développement de l'application de l'unité logique du SIS

Comme mentionné précédemment, l'unité logique du SIS a utilisé un progiciel de développement du logiciel d'application basé sur les langages de la CEI 61131-3. Le logiciel supporte trois des langages de la CEI 61131-3: texte structuré, à contacts et bloc fonctionnel. Des normes de codage distinctes sont nécessaires pour chaque langage. La liste d'instructions n'a pas été incluse puisqu'elle est similaire à celle du langage assembleur et pas appropriée pour les programmeurs d'application. Ceci est cohérent avec le Tableau C.1 de la CEI 61508-7.

Un certain nombre de restrictions supplémentaires ont été apportées aux définitions des langages de la CEI 61131-3, cohérentes avec les exigences décrites dans la CEI 61508-3 (7.4.4 et Tableau A.3) et dans la CEI 61508-7 (Article C.4). Celles-ci comprennent:

a) Hardware integration

This consists of the installation of the SIS logic solver into cabinets with the appropriate termination panels for connecting the process signals to the logic solver I/O modules. Power supplies and power distribution for the logic solver and field devices are also normally included.

b) Application logic definition

The SIS logic solver integration services may also define the detailed logic by working closely with customer engineers. The application logic for each safety instrumented function is defined taking into account the sensor and final element redundancy. The interface for testing and maintenance of the SIS while the process is in operation is also defined to meet the customer's operational requirements. Additional non-safety critical logic may also be included, but is strictly segregated and designed to the same standard as the safety function.

c) Application software implementation and hardware configuration

The SIS logic solver safety certified application software development package is used to configure the SIS logic solver I/O and communication hardware. The application software for each safety instrumented function as well as non-critical application software are also implemented and tested.

d) Factory acceptance testing

Many customers conduct a factory acceptance test to check the correct operation of the hardware and application software before it is shipped to the plant. The hardware and application software are thoroughly tested by the customer's engineers and other operating personnel.

e) Installation of SIS at customer site

Either supplier installation or installation supervision is provided at plant site.

f) Site acceptance testing

Each sensor and final element interface into the SIS logic solvers is checked for proper operation and calibration. Such items as the overall application software, bypass functions for maintenance, are re-tested.

g) Application software and hardware modifications

After initial installation and operation, application software and hardware modifications are implemented using strict plant-approved modification procedures.

D.2 SIS logic solver application development software

As mentioned earlier, the SIS logic solver utilized an application software development package based upon the IEC 61131-3 languages. The software supports three of the IEC 61131-3 languages: structured text, ladder diagram and function block. Separate coding standards are necessary for each language. Instruction List was not included since it is similar to assembly language and is not suited for application programmers. This is consistent with Table C.1 in IEC 61508-7.

A number of additional restrictions were placed upon the IEC 61131-3 language definitions consistent with the requirements outlined in IEC 61508-3 (7.4.4 and Table A.3) and IEC 61508-7 (Clause C.4). These include the following.

a) La CEI 61131-3 défini 20 types de données (BOOL, SINT, INT, DINT, LINT, USINT, UINT, UDINT, ULINT, REAL, LREAL, TIME, DATE, TOD, DT, STRING, BYTE, WORD, DWORD, LWORD). Il convient de noter qu'il y a seulement 8 types de données de nombres entiers. La prise en charge de tous ces types de données rend nécessaire également de pouvoir accepter des douzaines de fonctions de conversion et de troncature. Pour les applications de sécurité plusieurs de ces types de données ne sont pas nécessaires. Le nombre de types de données reconnus a été limité à onze (11). Pour le langage particulier des applications de sécurité, les types choisis de données proposés ont été BOOL, INT, DINT, DWORD, REAL, LREAL, STRING, TIME, DATE, TOD, et DT. Cette décision est cohérente avec les recommandations de la CEI 61508, de limiter le sous-ensemble du langage (voir le Tableau A.3 de la CEI 61508-3).

b) L'utilisation des «graphic execution control elements» (éléments de commande d'exécution graphique) de la CEI 61131-3 (par exemple, sauts inconditionnels, sauts conditionnels, retours inconditionnels et retours conditionnels) n'ont pas été supportés, du fait qu'ils peuvent conduire à faire une boucle et à faire une dérivation fortuite des éléments qui devraient être exécutés (voir C.4.6 de la CEI 61508-7).

c) Un certain nombre d'instructions en langage de texte structuré n'ont pas été prises en compte du fait qu'elles peuvent entraîner une boucle, (par exemple, FOR...END_FOR, WHILE...END_WHILE, et REPEAT...END_REPEAT).

d) Une limitation a été imposée de telle manière que le langage ne permet pas à plusieurs programmes d'écrire dans la même variable globale. De nombreux programmes peuvent lire une variable globale, mais afin d'empêcher des conflits et des écrasements, un seul programme peut écrire dans une variable globale. En outre, le logiciel de programmation de l'application donne un avertissement si plusieurs écritures sont programmées accidentellement.

e) Il convient que le logiciel de programmation définisse clairement l'ordre d'exécution de tous les éléments d'un programme. Les langages ont un algorithme qui détermine l'ordre d'exécution et affiche l'ordre d'exécution de chaque élément exécutable.

f) Il convient que le logiciel de programmation prévoit la séparation du logiciel critique de sécurité et du logiciel critique non sécuritaire. Le logiciel fournit au programmeur des possibilités pour définir les programmes de sécurité et les programmes non sécuritaires. Il fournit également des possibilités pour définir les variables de sécurité et les variables non sécuritaires. Les programmes non sécuritaires ne peuvent pas écrire dans des variables de sécurité.

g) L'utilisation des variables VAR_IN_OUT s'est avéré très difficile à comprendre pour la plupart des utilisateurs de l'application. L'utilisation des variables VAR_IN_OUT nécessite d'être très bien documentée, sinon le langage de programmation ne devrait pas pouvoir les supporter.

D.3 Normes de codage pour le programmeur de l'application

Afin d'assurer le développement d'un logiciel d'application sûr, il convient d'établir des normes de codage pour le programmeur de l'application. Un certain nombre de directives, utilisables par les programmeurs de l'application lorsqu'ils développent le logiciel d'application avec ce logiciel de développement particulier, sont données ci-après:

a) Il convient que le programmeur de l'application utilise des langages de variabilité limitée (langage en blocs fonctionnels ou langage à contacts) pour mettre en oeuvre les fonctions instrumentées de sécurité. Il convient même de restreindre ces langages (voir l'Article D.2 ci-dessus concernant le sous-ensemble du langage).

b) Le texte structuré (ST) est un langage de variabilité totale, et il convient d'en limiter son utilisation. Il convient d'en limiter l'usage à la mise en oeuvre des fonctions et des blocs fonctionnels, dans la mesure du possible. Cette restriction a été mise en place de manière que le personnel opérationnel non compétent en matière de programmation comprenne le programme de sécurité.

a) The IEC 61131-3 standard defines twenty data types (BOOL, SINT, INT, DINT, LINT, USINT, UINT, UDINT, ULINT, REAL, LREAL, TIME, DATE, TOD, DT, STRING, BYTE, WORD, DWORD, LWORD). It should be noted that there are 8 integer data types alone. The support of all these data types also necessitates the support of dozens of conversion and truncation functions. For safety applications many of these data types are not necessary. The number of data types supported was limited to eleven (11). For the particular language the chosen data types provided were BOOL, INT, DINT, DWORD, REAL, LREAL, STRING, TIME, DATE, TOD, and DT. This decision is consistent with the IEC 61508 recommendations to limit the language subset (see Table A.3 in IEC 61508-3).

b) The use of IEC 61131-3 graphic execution control elements (for example, unconditional jumps, conditional jumps, unconditional returns and conditional returns) were not supported since they can lead to looping and unintended bypassing of elements that should be executed (see C.4.6 in IEC 61508-7).

c) A number of structured text language statements were not supported since they can cause looping (for example FOR...END_FOR, WHILE...END_WHILE and REPEAT...END_REPEAT).

d) A limitation was imposed so that the language does not allow multiple programs to write into the same global variable. Many programs can read a global variable but in order to prevent conflicts and overwriting only one program can write into a global variable. In addition, the application programming software provides a warning if multiple writes are programmed accidentally.

e) The programming software should unambiguously define the execution order of all elements in a program. The languages have an algorithm that determines the execution order and displays the execution order on each executable element.

f) The programming software should provide for the separation of safety critical and non-safety critical software. The software provides the programmer with the capability to define safety programs and non-safety programs. It also provides the capability to define safety and non-safety variables. Non-safety programs cannot write into safety variables.

g) The use of VAR_IN_OUT variables has been found to be very confusing to most application users. The use of the VAR_IN_OUT variables needs to be very thoroughly documented, or the programming language should not support them.

D.3 Coding standards for the application programmer

In order to ensure the development of safe application software, coding standards should be established for the application programmer. Following are a number of guidelines for use by application programmers when developing application software with this particular development software:

a) The application programmer should use the limited variability languages (function block diagram or ladder diagram) to implement the safety instrumented functions. Even these languages should be restricted (see Clause D.2 above on language subset).

b) Structured text (ST) is a full variability language, and its use should be limited. The usage should be limited to the implementation of functions and function blocks wherever possible. This restriction was implemented so that operational personnel not proficient in programming would understand the safety program.

c) Il convient de limiter la taille des programmes à une taille raisonnable. Il convient de séparer les fonctions instrumentées de sécurité, pour différentes unités de processus, en programmes distincts. Dans le meilleur des cas, il convient qu'un programme ne contienne qu'un nombre restreint de fonctions instrumentées de sécurité pour une seule unité de processus.

d) Il convient d'éviter l'attribution d'alias (aliasing). Par exemple, si le logiciel de programmation supporte les tableaux, il convient que les programmes utilisant les tableaux vérifient les pointeurs de tableau pour s'assurer qu'ils sont dans la plage valide.

e) Lorsque l'application inclut une logique critique non sécuritaire, ainsi qu'une logique critique de sécurité, il convient que la logique critique non sécuritaire soit dans des programmes distincts et il convient d'utiliser les règles de séparation incorporées dans le programme.

D.4 Autres exigences pour la configuration/la programmation et les systèmes exécutables pour les applications de sécurité

Le logiciel de programmation de l'application présente un certain nombre de fonctionnalités qui permettent l'accès de l'utilisateur à des informations de l'unité logique du SIS. Cependant, il est nécessaire d'assurer la sécurité du logiciel développé et de permettre à l'utilisateur de vérifier le logiciel quant à son fonctionnement correct. Quelques-unes de ces fonctionnalités sont décrites ci-dessous:

a) Le logiciel de programmation comporte un système de sécurité qui limite l'accès de l'ensemble des utilisateurs aux seules fonctions utiles à leurs postes (par exemple, directeur de l'entreprise, directeur du site, chef de projet, ingénieur de projet, chef programmeur, programmeur, opérateur). Chaque utilisateur ouvre une session dans le système avec un nom et un mot de passe et peut ensuite travailler au niveau fonctionnel qui lui est assigné. Le système de sécurité comporte également un niveau utilisateur pour la programmation de sécurité et d'autres niveaux pour la programmation non sécuritaire, du fait que les sociétés des utilisateurs peuvent vouloir restreindre l'accès aux modifications des programmes de sécurité, à quelques personnes du site.

b) Des fonctions protégées ou verrouillées et des bibliothèques sont fournies et le programmeur ne peut pas y accéder ou les modifier. Ceci garantit que des bibliothèques qui ont été certifiées ou complètement testées ne peuvent pas être modifiées sans que cela soit approuvé par une demande formelle de modification. Le système de sécurité permet à l'utilisateur de définir une personne de haut niveau pouvant accéder aux bibliothèques et les modifier (typiquement un directeur de l'entreprise ou de site).

c) Le logiciel de programmation affecte aussi un numéro de version à tous les éléments du projet en cours de développement. Tout changement de la configuration du système, de fonction, de bloc fonctionnel, ou du programme a comme conséquence la modification du numéro de version pour l'élément considéré. Ceci permet aux utilisateurs de savoir rapidement si leur documentation est à jour ou non et leur permet de concentrer les tests sur les éléments qui ont été modifiés. Des fonctions de comparaison de version sont incluses, de façon que les utilisateurs puissent vérifier toutes les modifications, y compris les modifications involontaires. Il convient que ces fonctions de comparaison incluent toutes les modifications de la base de données globale de nom d'étiquette et de la liste d'exécution du programme.

d) Le logiciel donne la sécurité des fichiers en calculant et en vérifiant les contrôles par redondance cyclique sur tous les flux de données stockés dans la l'arborescence des fichiers non développée, du projet de l'application.

e) L'unité logique du SIS donne l'accès à ses informations de diagnostic et par conséquent le programmeur peut prendre les mesures appropriées, basées sur l'état de l'unité logique.

f) L'unité logique du SIS fournit un environnement d'exécution qui donne des exceptions arithmétiques, ainsi le programmeur peut vérifier que les opérations arithmétiques sont correctes.

c) The size of the programs should be restricted to a reasonable size. Safety instrumented functions for different process units should be in separate programs. Ideally a program should only contain a small number of safety instrumented functions for one process unit.

d) Aliasing should be avoided. For example, if the programming software supports arrays, the programs using the arrays should check the array pointers to make sure they are in the valid range.

e) When the application includes non-safety critical logic as well as the safety critical logic, the non-safety critical logic should be in separate programs and utilise the separation rules incorporated in the program.

D.4 Other requirements for configuration/programming and run-time systems for safety applications

The application programming software provides a number of features that allow user access to SIS logic solver information. However, it is necessary to ensure the security of the developed software and to allow the user to check the software for proper operation. A few of these features are outlined below:

a) The programming software provides a security system that restricts all users to only those functions that are commensurate with their duties (for example, corporate manager, site manager, project manager, project engineer, senior programmer, programmer, operator). Each user logs into the system with a name and password and can then work at their assigned functional level. The security system also provides a user level for safety programming and another for non-safety programming since the user companies may want to restrict the changing of safety programs to a few persons at the site.

b) Protected or locked functions and libraries are provided and the programmer cannot access or change them. This ensures that libraries that have been certified or thoroughly tested cannot be modified unless approved by a formal modification request. The security system allows the user to define a high level person that can access and change the libraries (typically a corporate or site manager).

c) The programming software also provides a version number on all elements in the project being developed. Any change of the system configuration, function, function block, or program results in the version number being changed for that element. This allows the user to quickly know if their documentation is out of date and allows them to concentrate the testing on those items that have been modified. Version comparison functions are included so users can check all changes, including unintentional changes. These comparison functions should include any changes in the global tag name database and the program execution list.

d) The software provides file security by computing and checking the cyclic redundancy checks on all data streams stored in the compound file structure of the application project.

e) The SIS logic solver provides access to its diagnostic information and hence the programmer can take appropriate actions based upon the status of the logic solver.

f) The SIS logic solver provides a run-time environment that provides arithmetic exceptions so the programmer can check for proper arithmetic operations.

g) Le logiciel de programmation donne la capacité d'émuler tous les programmes développés sur la station de travail de programmation. Ceci permet au programmeur de vérifier tout le logiciel développé «hors-ligne» avant qu'il ne soit chargé dans l'unité logique du SIS. Il convient que cette fonctionnalité soit obligatoire pour les cas où une modification est faite au programme «en ligne», alors que le système est en exploitation.

h) Le logiciel supporte le DDE (l'échange dynamique de données), qui peut être utilisé pour interfacer le logiciel de simulation. Ceci donne la possibilité de réaliser des essais supplémentaires «hors-ligne» du logiciel d'application, avant qu'il ne soit chargé dans le contrôleur de sécurité.

D.5 Hypothèses

Cet article traite des hypothèses associées au matériel et au logiciel et utilisées pour développer le logiciel d'application. La documentation et les procédures sont également commentées.

1) L'unité logique du SIS et ses modules d'E/S associés ont été évalués par un tiers et se sont révélés être conformes à la CEI 61508. L'étendue de la certification CEI 61508 attribuée par le tiers est à utiliser comme un composant dans les fonctions instrumentées de sécurité de SIL3.

2) Les langages constituent un sous-ensemble de variabilité limitée du langage en blocs fonctionnels (FBD), du langage à contacts (LD), et du langage en texte structuré (ST) de la CEI 61131-3. Toutes les fonctions et tous les blocs fonctionnels donnés dans les bibliothèques d'application ont un attribut qui identifie si la fonction peut être utilisée pour la sécurité ou est limitée exclusivement à ce qui n'est pas relatif à la sécurité. Seules des fonctions et les blocs fonctionnels avec attribut de sécurité peuvent être utilisés pour mettre en oeuvre des fonctions instrumentées de sécurité dans des programmes d'application annoncés avec attribut de sécurité. Les programmes d'application annoncés avec attribut non relatif à la sécurité peuvent utiliser des fonctions et des blocs fonctionnels avec attribut non relatif à la sécurité et attribut de sécurité.

3) Tous les langages de programmation CEI 61131-3 supportés et les bibliothèques de fonctions et de blocs fonctionnels avec attribut de sécurité ont été certifiés conformes à la CEI 61508.

4) Toutes les restrictions d'organismes de certification et toutes les procédures opérationnelles sont données dans la documentation utilisateur.

5) Pour les essais périodiques de tous les éléments du SIS, une méthodologie pour la maintenance prioritaire est en général nécessaire pour permettre les essais «en ligne», sans arrêter le processus en cours.

6) Toutes les fonctions d'intégration du système sont réalisées en utilisant les procédures ISO 9000 ou des procédures équivalentes.

g) The programming software provides the ability to emulate all of the programs developed on the programming workstation. This allows the programmer to check all of the developed software off-line before it is loaded into the SIS logic solver. This feature should be mandatory for cases where a change is made to the on-line program while the system is in operation.

h) The software supports DDE (dynamic data exchange) which can be used to interface to simulation software. This provides the capability for additional off-line testing of the application software before it is loaded into the safety controller.

D.5 Assumptions

This clause discusses the assumptions associated with the hardware and software used to develop the application software. Documentation and procedures are also discussed.

1) The SIS logic solver and its associated I/O modules have been assessed by a third party and found to be compliant to the IEC 61508 series. The scope of the IEC 61508 series certification awarded by the third party is for use as a component in SIL 3 safety instrumented functions.

2) The languages are a limited variability subset of the IEC 61131-3 function block diagram (FBD), ladder diagram (LD), and structured text (ST) languages. All functions and function blocks provided in the application libraries have an attribute that identifies whether the function can be used for safety or is restricted to non-safety only. Only functions and function blocks with the safety attribute can be used to implement safety instrumented functions in application programs designated with the safety attribute. Application programs designated with the non-safety attribute can use functions and function blocks with the non-safety attribute and the safety attribute.

3) All of the supported IEC 61131-3 programming languages and libraries of functions and function blocks with the safety attribute have been certified for compliance to the IEC 61508 series.

4) All certifying organization restrictions and operating procedures are provided in the user documentation.

5) For periodic testing of all elements of the SIS, a methodology for maintenance override is typically necessary to allow on-line testing without shutting down the process under control.

6) All system integration functions are performed using ISO 9000 or equivalent procedures.

Annexe E
(informative)

Exemple de développement de dispositifs de diagnostic configurés extérieurement pour une unité logique à électronique programmable (PE) configurée pour la sécurité

Il convient que les unités logiques à électronique programmable (PE) validées en utilisation fassent la preuve de diagnostics suffisants réalisés à l'étape de la conception.. Les diagnostics peuvent être basés sur le logiciel ou sur le matériel et il convient qu'ils couvrent l'ensemble de l'unité logique, y compris des modules d'entrée, le processeur principal, les modules de sortie et les communications.

Un canevas, qui peut être utilisé pour fournir les diagnostics relatifs aux unités logiques à PE configurées pour la sécurité, est donné ci-après.

E.1 Dispositifs de diagnostic configurés intérieurement

Les unités logiques à PE dans le domaine des processus industriels ont des dispositifs de diagnostics configurés intérieurement. Ils sont nommés «horloges de surveillance internes» (Internal Watchdog Timer ou IWDT) dans cette annexe. Les IWDT comprennent le logiciel, le matériel et les sous-systèmes de communication de diagnostic fournis par le constructeur, au sein de l'unité logique à PE.

Il convient que les unités logiques à PE, pour les applications de SIF, donnent des diagnostics pour tous les éléments de l'unité logique à PE. Un système d'IWDT peut offrir des options sélectionnables par l'utilisateur s'étendant de l'arrêt d'une carte d'entrée ou de sortie jusqu'à l'arrêt total du système. Les dispositifs de diagnostic IWDT vérifient les points que le constructeur de l'unité logique considère comme étant les plus importants. Les limitations d'une IWDT peuvent inclure

– une défaillance potentielle de mode commun dans laquelle l'IWDT tombe en panne en raison de la même cause que l'unité logique, avec pour conséquence l'incapacité de l'IWDT à remplir ses fonctions de diagnostic;
– l'implémentation peut ne pas fournir à l'utilisateur les informations de diagnostic relatives à l'état d'anomalie de l'unité logique;
– l'incapacité à surveiller l'ensemble de l'unité logique à PE, y compris les E/S, les processeurs principaux et les communications;
– l'incapacité à surveiller les modules du logiciel d'application et l'exécution.

E.2 Dispositifs de diagnostic configurés extérieurement

– Les limitations inhérentes aux IWDT peuvent nécessiter l'adjonction d'horloges de surveillance externes (External Watchdog Timer ou EWDT) pour des unités logiques à PE exécutant des fonctions instrumentées de sécurité. L'utilisation des EWDT n'élimine nullement le besoin d'IWDT pour les fonctions instrumentées de sécurité.
– Des exemples de dispositifs d'EWDT fréquemment utilisés sont: un moniteur de roto-pulsateur ou un moniteur électronique de synchronisation. Sous sa forme la plus élémentaire, l'EWDT est continuellement pilotée par la logique d'application située dans le logiciel d'application de l'unité logique à PE. Le concept généralement utilisé consiste à programmer plusieurs groupes d'instructions (qui sont fortement séparés dans les emplacements mémoire clés) pour générer d'une onde carrée avec la période souhaitée. Cette onde carrée est utilisée comme entrée de l'EWDT. La Figure 5 est un diagramme temporel qui montre la sortie pulsée de l'unité logique à PE et la sortie de l'EWDT.

Annex E
(informative)

Example of development of externally configured diagnostics for a safety-configured PE logic solver

Proven-in-use PE logic solvers should demonstrate sufficient diagnostics in the PE logic solver design. The diagnostics can be software or hardware based and should cover the entire logic solver, including input modules, main processor, output modules, and communications.

Following is a scheme that may be used to provide diagnostics for safety configured PE logic solvers.

E.1 Internally configured diagnostics

Industrial process sector PE logic solvers have internally configured diagnostics. They are referred to as internal watchdog timers (IWDT) in this annex. IWDTs include software, hardware, and communication diagnostic subsystems provided by the manufacturer, within the PE logic solver.

PE logic solvers for SIF applications should provide diagnostics for all elements of the PE logic solver. An IWDT system may provide user selectable options ranging from the shutdown of an input or output card to total shutdown of the system. IWDT diagnostics check items the logic solver manufacturer considers most important. The limitations of an IWDT may include:

- potential common mode failure in which the IWDT fails due to the same cause as the logic solver, resulting in the inability of the IWDT to perform its diagnostic functions;
- implementation may not provide the user with diagnostic information related to the logic solver fault status;
- inability to monitor the entire PE logic solver, including I/O, main processors, and communications;
- inability to monitor the application software modules and execution.

E.2 Externally configured diagnostics

- The limitations inherent in IWDTs may require the addition of external watchdog timers (EWDTs) for PE logic solvers performing safety instrumented functions. The use of EWDTs in no way eliminates the need for IWDTs for safety instrumented functions.
- Examples of EWDT devices frequently used are a rotopulsor monitor or an electronic timing monitor. In its most basic form, the EWDT is continuously pulsed by application logic located in the PE logic solver application software. The concept generally employed is to program several groups of instructions (that are widely separated in key memory locations) to generate a square wave with a desired period. This square wave is used as the input to the EWDT. Figure E.1 is a timing diagram that shows the pulsed output of the PE logic solver and the output of the EWDT.

– Cette onde carrée pilote une sortie de l'unité logique à PE en commutation tout ou rien en suivant la séquence temporelle correcte, qui maintient la sortie de l'EWDT activée. Notez que l'EWDT a habituellement des fonctions intégrées de temporisation réglable du retard de l'état «activé» et du retard de l'état «désactivé». Les réglages du temporisateur de retard de l'état «activé» et de retard de l'état «désactivé» sont effectués de telle manière qu'il convient qu'aucun retard ne soit en dépassement de temps. Si l'EWDT est en dépassement de temps, la sortie de l'EWDT tombe au repos, et le SIF peut être arrêté et/ou une alarme peut être déclenchée. Les impulsions de cette onde carrée peuvent être changées en modifiant le programme d'application au niveau du générateur d'onde carré.

– Les fonctionnalités de conception supplémentaires, lorsqu'un dispositif de diagnostic EWDT est mis en oeuvre, comprennent les éléments indiqués ci-dessous.

  – La génération de l'onde carrée de l'unité logique à PE pour l'EWDT, utilise le même jeu d'instructions que celui qui est utilisé dans le logiciel d'application de la SIF;

  – Des entrées dédiées de l'unité logique à PE surveillent l'état de la ou des entrées des bus de l'unité logique pour détecter les dysfonctionnements;

  – Une distribution du programme de l'EWDT sur divers emplacements mémoire de l'unité logique à PE surveillera mieux la fonctionnalité globale de la mémoire.

  – Une transmission de l'onde carrée générée dans tout le système de communication de l'unité logique à PE pour améliorer les diagnostics de communication de cette dernière.

  – L'éventuel besoin de boutons de réinitialisation. Un bouton «réinitialisation» sera requis si l'EWDT est verrouillé à l'état désactivé, à la mise en marche ou sur un arrêt. Considérez à la fois l'EWDT et l'IWDT en développant le circuit de réinitialisation;

  – L'éventuel besoin de boutons de test. Un bouton «test» peut être souhaitable pour vérifier la fonctionnalité de l'EWDT;

  – Des sorties dédiées de l'unité logique à PE surveillent l'état de la (des) sortie(s) des bus de l'unité logique à PE pour détecter les dysfonctionnements;

  – Un dispositif anti-surtensions pour amortir l'interaction inductive de tout contact de relais électromécanique vis-à-vis de l'électronique. Examiner l'application de exigences supplémentaires de traitement de l'alimentation électrique comme:

    – protection contre les sous-tensions;

    – suppression du bruit électrique;

    – protection contre la foudre.

    – développement d'alarme de sorte que le déclenchement de l'EWDT et de l'IWDT puisse être déterminé.

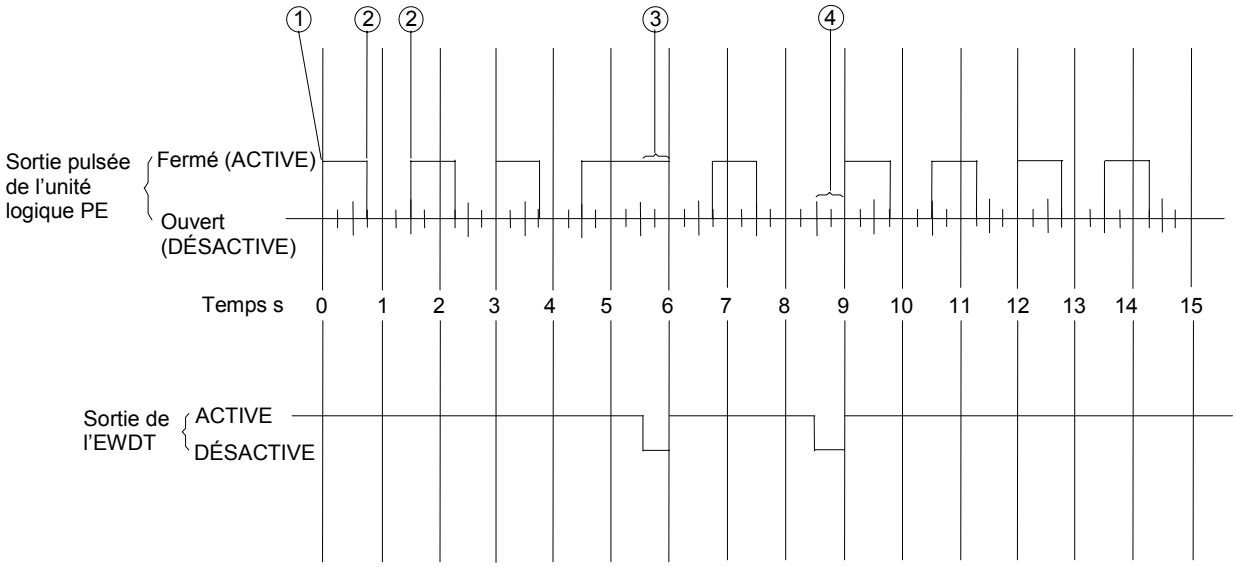
E.3 Document de référence

CCPS, «*Guidelines for Safe Automation of Chemical Processes*» (*Directives relatives à la sécurité des automatismes des processus chimiques*), AIChE, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0554-1, 1993.

- This square wave drives a PE logic solver output on and off in the correct timing sequence that keeps the EWDT output energized. Note that the EWDT typically has built-in adjustable ON-delay and OFF-delay timer functions. The ON-delay and OFF-delay timer settings of the EWDT are set so that neither delay should time out. If the EWDT times out, the EWDT output drops out, and the SIF may be shut down and/or alarmed. The pulses in this square wave can be varied by changing the application program in the square wave generator.
- Additional design features to be considered when implementing EWDT diagnostics include:
  - PE logic solver square wave generation for the EWDT utilizes the same instruction set used in the SIF application software;
  - Dedicated PE logic solver inputs to monitor the state of the logic solver input(s) buses to detect abnormal operation;
  - Distribution of the EWDT program across various memory locations of the PE logic solver that will best monitor total memory functionality.
  - Transmission of the generated square wave throughout the PE logic solver communication system to improve PE logic solver communication diagnostics.
  - The possible need for reset buttons. A reset button will be required if the EWDT is interlocked down at start-up or upon shutdown. Consider both the EWDT and IWDT when developing the reset circuit;
  - The possible need for test buttons. A test button may be desirable to verify EWDT functionality;
  - Dedicated PE logic solver outputs to monitor the state of the PE logic solver output(s) buses to detect abnormal operation;
  - A surge suppressor to dampen the inductive interaction to the electronics from any electro-mechanical relay contact. Review the application for additional power line conditioning requirements such as:
    - undervoltage protection;
    - electrical noise suppression;
    - lightning protection;
    - alarm development so that either EWDT and IWDT initiation can be determined.

E.3 Reference

CCPS, "*Guidelines for Safe Automation of Chemical Processes*", AIChE, 345 East 47th Street, New York, New York 10017, ISBN 0-8169-0554-1, 1993.



NOTES:

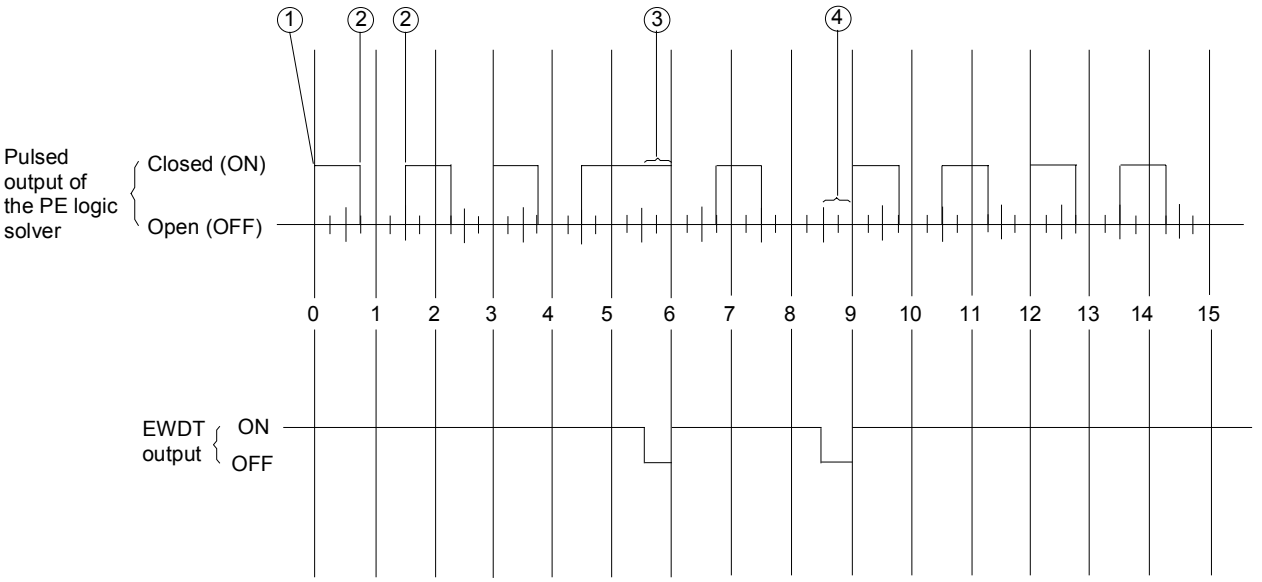
① La fermeture du circuit de commande active la sortie.

② L'ouverture et la re-fermeture du circuit de commande avant que l'intervalle de temps établi (supposé être établi à 1 s) ne soit terminé, maintient la sortie de l'EWDT activée. La sortie reste activée tant que les impulsions surveillées continuent à donner au moins une transition par intervalle de temps établi.

③ Si la commande surveillée se maintient plus longtemps que le temps indiqué (③), la sortie de l'EWDT se désactive.

④ Si la commande surveillée se maintient moins longtemps que le temps indiqué (④), la sortie de l'EWDT se désactive.

Figure E.1 – Diagramme temporel de l'EWDT



IEC 1832/03

Key

① Closing the control circuit energizes the output.

② Opening and reclosing the control circuit before the set time interval (assume set at 1 second) is complete keeps the EWDT output energized. The output remains energized as long as the monitored pulsing continues to provide at least 1 transition per set time interval.

③ If the monitored control stays on longer than the preset time (③), the EWDT output de-energizes.

④ If the monitored control stays off longer than the preset time (④), the EWDT output de-energizes.

Figure E.1 – EWDT timing diagram

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-7556-0

ICS 13.110; 25.040.01

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND