NORME INTERNATIONALE

ISO 13849-2

Première édition
2003-08-15

Sécurité des machines — Parties des systèmes de commande relatifs à la sécurité —

Partie 2: Validation

Safety of machinery — Safety-related parts of control systems — Part 2: Validation

Numéro de référence
ISO 13849-2:2003(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 13849-2 a été élaborée par le Comité européen de normalisation (CEN) en collaboration avec le comité technique ISO/TC 199, *Sécurité des machines*, conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Tout au long du texte du présent document, lire «… la présente Norme européenne …» avec le sens de «… la présente Norme internationale …».

L'ISO 13849 comprend les parties suivantes, présentées sous le titre général *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité*:

— *Partie 1: Principes généraux de conception*

— *Partie 2: Validation*

— *Partie 100: Lignes directrices pour l'utilisation et l'application de l'ISO 13849-1*

Sommaire

Page

Avant-propos

Le présent document EN ISO 13849-2:2003 a été élaboré par le Comité Technique CEN/TC 114 “Sécurité des machines”, dont le secrétariat est tenu par le DIN, en collaboration avec le Comité Technique ISO/TC 199 “Sécurité des machines”.

Cette Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en février 2004, et toutes les normes nationales en contradiction devront être retirées au plus tard en février 2004.

Le présent document a été élaboré dans le cadre d'un mandat donné au CEN par la Commission Européenne et l'Association Européenne de Libre Échange et vient à l'appui des exigences essentielles de la (des) Directive(s) CE.

Les Annexes A à D sont informatives et sont structurées comme indiqué au Tableau 1.

Tableau 1 — Structure des articles des Annexes A à D

Annexe	Technologie	Liste des principes de sécurité de base	Liste des principes de sécurité éprouvés	Liste des composants de sécurité éprouvés	Liste des défauts et exclusions de défauts
		Article			
A	Mécanique	A.2	A.3	A.4	A.5
B	Pneumatique	B.2	B.3	B.4	B.5
C	Hydraulique	C.2	C.3	C.4	C.5
D	Électrique (y compris électroniques)	D.2	D.3	D.4	D.5

Le présent document comprend une Bibliographie.

L’EN ISO 13849 comprend les parties suivantes, présentées sous le titres général "Sécurité des machines – Parties de systèmes de commande relatives à la sécurité" :

Partie 1 : Principes généraux de conception.

Partie 2 : Validation.

Partie 100 : Lignes directrices pour l'utilisation et l'application de l'EN ISO 13849-1.

Selon le Règlement Intérieur du CEN/CENELEC, les instituts de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Luxembourg, Malte, Norvège, Pays-Bas, Portugal, République Tchèque, Royaume-Uni, Slovaquie, Suède et Suisse.

Introduction

Pour l'utilisation dans l'Union Européenne, la présente partie de l'EN ISO 13849 a le statut d'une norme de sécurité générique (type B1).

La présente Norme européenne spécifie le processus de validation, comportant à la fois l'analyse et les essais des fonctions et catégories de sécurité des parties des systèmes de commande relatives à la sécurité. Les descriptions des fonctions de sécurité et les prescriptions relatives aux catégories sont données dans l'EN 954-1 (ISO 13849-1) qui traite des principes généraux de conception. Certaines prescriptions pour la validation sont générales et d'autres sont particulières à la technologie utilisée. L'EN ISO 13849-2 spécifie également les conditions dans lesquelles il convient d'effectuer la validation par essais des parties de systèmes de commande relatives à la sécurité.

L'EN 954-1 (ISO 13849-1) spécifie les prescriptions de sécurité et donne des indications sur les principes de conception [voir EN 292-1:1991 (ISO/TR 12100-1:1992) 3.11] des parties de systèmes de commande relatives à la sécurité. Pour ces parties, elle spécifie des catégories et décrit les caractéristiques des fonctions de sécurité indépendamment du type d'énergie utilisée. Des conseils supplémentaires concernant la norme EN 954-1 (ISO 13849-1) sont donnés dans le guide CR 954-100 (ISO/TR 13849-100).

Le respect des prescriptions peut être validé par toute combinaison d'analyse (voir article 4) et d'essais (voir article 5). Il convient de commencer cette analyse dès que possible pendant le processus de conception.

1 Domaine d'application

La présente Norme européenne spécifie les procédures et conditions à suivre pour la validation par analyse et par essais :

— des fonctions de sécurité assurées ; et

— de la catégorie atteinte.

par les parties de système de commande relatives à la sécurité en conformité avec l'EN 954-1 (ISO 13849-1), en utilisant le raisonnement de conception fourni par le concepteur.

La présente Norme européenne ne donne pas de prescriptions complètes de validation pour les systèmes électroniques programmables et peut par conséquent nécessiter l'utilisation d'autres normes.

NOTE Le CEN/TC 114/WG 6 propose de traiter avec plus de détail la validation des systèmes électroniques programmables pendant l'élaboration de la révision de l'EN 954-1 (ISO 13849-1). Une norme d'application pour les machines (projet CEI 62061), basée sur la CEI 61508, est en préparation. Des prescriptions pour les systèmes électroniques programmables, incluant les logiciels embarqués, sont données dans la norme CEI 61508.

2 Références normatives

Cette Norme européenne comporte par référence datée ou non datée des dispositions d'autres publications. Ces références normatives sont citées aux endroits appropriés dans le texte et les publications sont énumérées ci-après. Pour les références datées, les amendements ou révisions ultérieurs de l'une quelconque de ces publications ne s'appliquent à cette Norme européenne que s'ils y ont été incorporés par amendement ou révision. Pour les références non datées, la dernière édition de la publication à laquelle il est fait référence s'applique (y compris les amendements).

EN 292-1:1991 (ISO/TR 12100:1992), *Sécurité des machines - Notions fondamentales, principes généraux de conception – Partie 1 : Terminologie de base, méthodologie.*

EN 954-1:1996 (ISO 13849-1:1999), *Sécurité des machines - Parties de systèmes de commande relatives à la sécurité – Partie 1 : Principes généraux de conception.*

3 Processus de validation

3.1 Principes de validation

Le but du processus de validation est de confirmer la spécification et la conformité de la conception des parties de système de commande relatives à la sécurité, dans le cadre des prescriptions de sécurité globales des machines.

La validation doit démontrer que chacune des parties relatives à la sécurité répond aux prescriptions de l'EN 954-1 (ISO 13849-1), en particulier :

— les caractéristiques de sécurité spécifiées des fonctions de sécurité assurées par cette partie, conformément au raisonnement de conception et ;

— les prescriptions de la catégorie spécifiée [voir EN 954-1:1996 (ISO 13849-1:1999) article 6].

Il convient que la validation soit effectuée par des personnes qui sont indépendantes de la conception de la (des) partie (s) relative (s) à la sécurité.

NOTE Une personne indépendantes ne signifie pas nécessairement qu'un essai de tiers est requis.

Il convient que le degré d'indépendance reflète la performance de la partie relative à la sécurité.

La validation consiste à mettre en œuvre l'analyse (voir article 4) et, si nécessaire, à faire des essais (voir article 5) conformément au plan de validation. La Figure 1 donne une vue d'ensemble du processus de validation. Le dosage entre l'analyse et/ou les essais dépend de la technologie.

Il convient que l'analyse soit entreprise aussi tôt que possible et en parallèle avec le processus de conception, de sorte que les problèmes puissent être corrigés précocement pendant qu'il est encore aisé de le faire, c'est-à-dire durant les phases 3 et 4 de l'EN 954-1:1996 (ISO 13849-1:1999), 4.3. Il peut être nécessaire de retarder certaines parties des analyses jusqu'à ce que la conception soit bien avancée.

Dans le cas de grands systèmes, en raison de la taille, de la complexité ou de l'intégration (à la machine) du système de commande, des dispositions particulières peuvent être adoptées pour :

— valider les parties de système de commande relatives à la sécurité séparément avant intégration y compris la simulation des signaux d'entrée et de sortie appropriés ;

— valider les effets de l'intégration des parties de systèmes de commande relatives à la sécurité au reste du circuit de commande dans le contexte de son utilisation dans la machine.

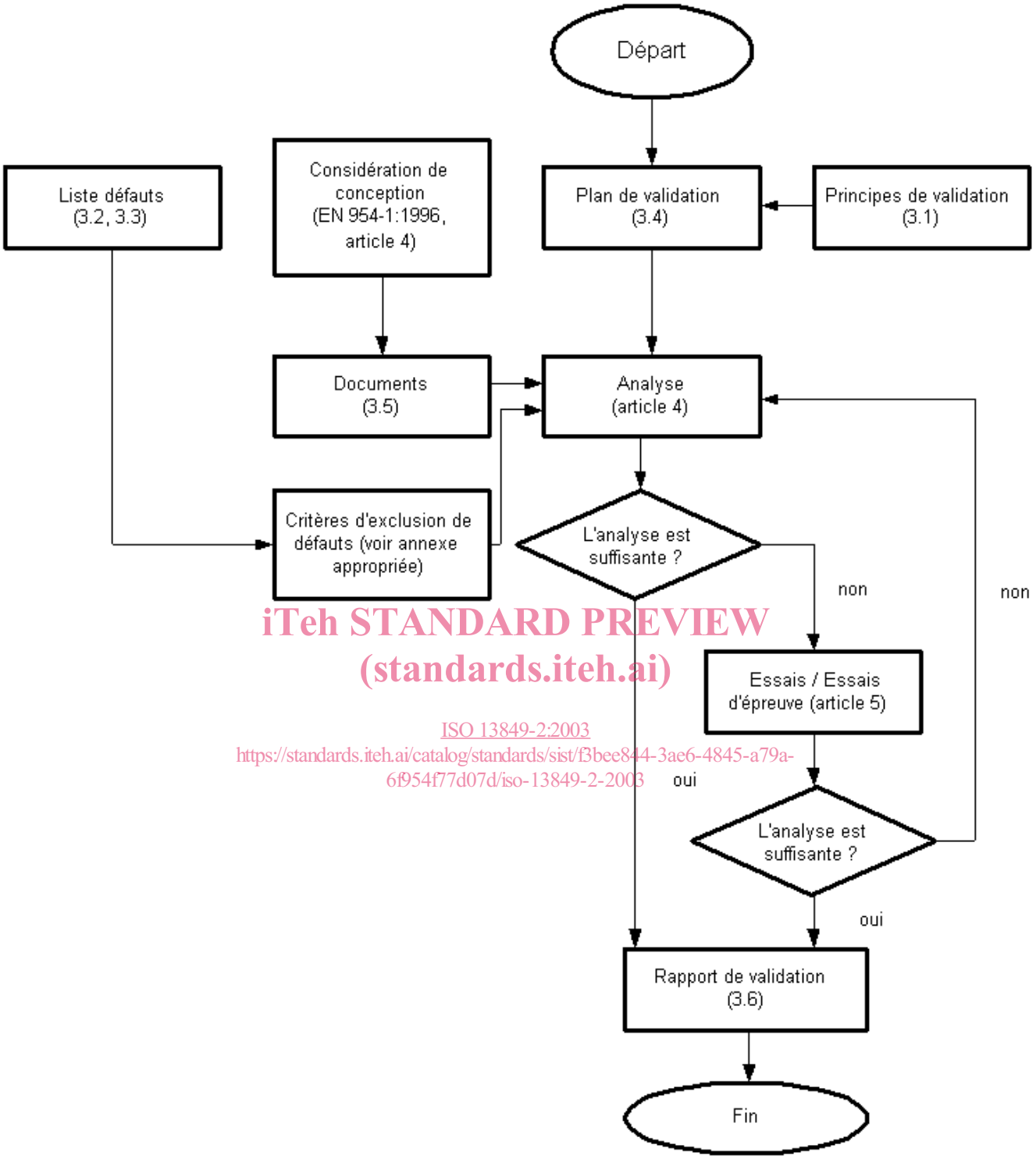

Figure 1 — Vue d'ensemble du processus de validation

3.2 Listes des défauts génériques

Le processus de validation nécessite la prise en compte du comportement de la (des) partie(s) relative(s) à la sécurité du système de commande pour tous les défauts à considérer. Une base pour la considération des défauts est donnée dans les listes de défauts des annexes informatives (A.5, B.5, C.5 et D.5), qui s'appuient sur l'expérience. Les listes des défauts génériques comportent :

— les composants/éléments à inclure, par exemple : les conducteurs/câbles (voir D.5.2) ;

— les défauts à prendre en compte, par exemple les courts-circuits entre conducteurs ;

— les exclusions de défauts autorisées ;

— une rubrique de remarques justifiant les exclusions de défauts.

Seuls les défauts permanents sont pris en compte.

3.3 Listes des défauts spécifiques

Une liste des défauts spécifiques se rapportant au produit doit être établie pour servir de document de référence au processus de validation de la (des) partie(s) relative(s) à la sécurité. La liste peut s'appuyer sur la(les) liste(s) générique(s) appropriée(s) figurant en annexe.

Lorsque la liste des défauts spécifiques se rapportant au produit est basée sur une (des) liste(s) générique elle doit mentionner :

— les défauts extraits de la(des) liste(s) générique(s) à inclure ;

— tout autre défaut pertinent à inclure mais non donné dans la liste générique (par exemple : défauts de mode commun) ;

— les défauts extraits de la(des) liste(s) générique(s) qu'il est possible d'exclure et qui peuvent au moins satisfaire aux critères indiqués dans la(les) liste(s) générique(s) [voir EN 954-1:1996 (ISO 13849-1:1999), 7.2] ;

et exceptionnellement

— tout autre défaut pertinent, figurant dans la liste générique mais non susceptible d'être exclu par la(les) liste(s) générique(s), ainsi que la justification de son exclusion et le raisonnement suivi pour parvenir à cette exclusion [voir EN 954-1:1996 (ISO 13849-1:1999), 7.2].

Lorsque cette liste n'est pas basée sur une(des) liste(s) générique(s) le concepteur doit donner le raisonnement pour les exclusions de défaut.

3.4 Plan de validation

Le plan de validation doit identifier et décrire les prescriptions de mise en œuvre du processus de validation des fonctions de sécurité spécifiées et de leurs catégories.

Le plan de validation doit également identifier les moyens à employer pour valider les fonctions de sécurité spécifiées et les catégories. Lorsque cela est approprié, il doit établir :

a) l'identité des documents de spécification ;

b) les conditions de fonctionnement et d'environnement ;

c) les principes de sécurité de base (voir A.2, B.2, C.2, et D.2) ;

d) les principes de sécurité éprouvés (voir A.3, B.3, C.3, et D.3) ;

e) les composants éprouvés (voir A.4 et D.4) ;

f) les hypothèses de défauts et les exclusions de défauts à prendre en compte, par exemple à partir des listes informatives de défauts de A.5, B.5, C.5, et D.5 ;

g) les analyses et les essais à appliquer.

Pour les parties relatives à la sécurité qui ont été validées précédemment pour une même application, une référence à cette précédente validation suffit.

3.5 Informations pour la validation

L'information requise pour la validation varie avec la technologie utilisée, la(les) catégorie(s) à démontrer, le raisonnement suivi lors de la conception du système et la contribution des parties relatives à la sécurité des systèmes de commande à la réduction des risques. Les documents contenant une information suffisante et issus de la liste ci-dessous doivent être inclus dans le processus de validation afin de démontrer la(les) catégorie(s) et la(les) fonction(s) de sécurité des parties de systèmes de commande relatives à la sécurité qui ont été réalisées :

a) spécification(s) des performances escomptées des fonctions de sécurité et des catégories ;

b) plans et spécifications, par exemple pour les parties mécaniques, hydrauliques et pneumatiques, cartes de circuits intégrés et cartes assemblées, câblage intérieur, enveloppe, matériaux, montage ;

c) schéma(s) fonctionnel(s) avec description fonctionnelle des blocs ;

d) schéma(s) de circuits y compris les interfaces/connexions ;

e) description fonctionnelle du(des) schéma(s) de circuits ;

f) diagrammes séquentiels des composants de commutation, signaux relatifs à la sécurité ;

g) description des caractéristiques pertinentes des composants préalablement validés ;

h) pour les autres parties relatives à la sécurité (sauf celles listées en g)), listes des composants avec désignation des éléments, valeurs nominales, tolérances, contraintes en fonctionnement, désignation du type, données relatives au taux de défaillance, fabricant des composants et toute autre donnée relative à la sécurité ;

i) analyse de tous les défauts pertinents (voir aussi 3.2) listés par exemple en A.5, B.5, C.5, et D.5, incluant la justification de toute exclusion de défauts ;

j) analyse de l'influence des matériaux traités ;

Informations spécifiques à la catégorie conformément au Tableau 2. Lorsque cela est approprié, la documentation relative aux logiciels doit inclure :

1) une spécification claire, et sans ambiguïté établissant les performances de sécurité que le logiciel doit réaliser, et

2) la preuve que le logiciel est conçu pour réaliser les performances de sécurité requises, et

3) les détails des essais (en particulier les rapports d'essais) effectués pour prouver que les performances de sécurité requises sont réalisées.

Tableau 2 — Prescriptions de documentation par catégories

Prescription de documentation	Catégorie pour laquelle la documentation est exigée				
	B	1	2	3	4
Principes de sécurité de base	X	X	X	X	X
Contraintes de fonctionnement prévues	X	X	X	X	X
Influences du matériau traité	X	X	X	X	X
Performances sous d'autres influences extérieures	X	X	X	X	X
Composants éprouvés	–	X	–	–	–
Principes de sécurité éprouvés	–	X	X	X	X
Procédure de contrôle de la (des) fonction(s) de sécurité	–	v	X	–	–
Intervalles de contrôle, lorsque spécifiés	–	–	X	–	–
Défauts uniques prévisibles pris en compte à la conception et méthode de détection utilisée	–	–	X	X	X
Défaillances de mode commun identifiées et mode de prévention	–	–	–	X	X
Exclusions de défauts uniques prévisibles	–	–	–	X	X
Défauts à détecter	–	–	X	X	X
Diversité des accumulations de défauts prises en compte à la conception	–	–	–	–	X
Manière dont la fonction de sécurité est assurée pour chaque défaut	–	–	–	X	X
Manière dont la fonction de sécurité est assurée pour chaque combinaison de défauts	–	–	–	–	X

NOTE Les catégories mentionnées dans le Tableau 2 sont celles données dans l'EN 954-1 (ISO 13849-1).

3.6 Rapport de validation

La validation par analyse et essais doit faire l'objet d'un rapport. Le rapport doit décrire le processus de validation de chaque prescription de sécurité. Il est possible de faire référence à de précédents rapports de validation, à condition qu'ils soient convenablement identifiés.

Pour toute partie relative à la sécurité qui n'a pas franchi une partie du processus de validation, le rapport de validation doit indiquer la(les) partie(s) des essais de validation et/ou des analyses qui a (ont) échoué.

4 Validation par analyse

4.1 Généralités

La validation des parties de systèmes de commande relatives à la sécurité doit être effectuée par analyse. Les données d'entrée de l'analyse sont :

— les phénomènes dangereux identifiés au cours de l'analyse sur la machine [voir EN 954-1:1996 (ISO 13849-1:1999), Figure 1] ;

— la fiabilité machine [voir EN 954-1:1996 (ISO 13849-1:1999), 4.2] ;

— l'architecture du système machine [voir EN 954-1:1996 (ISO 13849-1:1999), 4.2] ;

— les aspects qualitatifs, non quantifiable, influant sur le comportement du système [voir EN 954-1:1996 (ISO 13849-1:1999), 4.2] ;

— arguments déterministes.

La validation des fonctions de sécurité par analyse plutôt que par essais exige la formulation d'arguments déterministes. Les arguments déterministes diffèrent des autres justifications en cela qu'ils montrent que les propriétés exigées du système découlent logiquement d'une modélisation du système. De tels arguments peuvent être construits sur la base de notions simples, bien comprises, telles que la justesse d'un verrouillage mécanique.

NOTE Un argument déterministe est un argument, fondé sur des aspects qualitatifs (par exemple : qualité de fabrication, taux de défaillance, expérience d'utilisation). Cette analyse dépend de l'application. Cela et d'autres facteurs peuvent affecter les arguments déterministes.

4.2 Techniques d'analyse

Le choix d'une technique d'analyse dépend de l'objectif à atteindre. Deux types fondamentaux de techniques existent :

a) Les techniques descendantes (déductives) conviennent pour déterminer les événements déclencheurs qui peuvent conduire à des événements supérieurs identifiés et pour calculer la probabilité des événements supérieurs à partir de la probabilité des événements déclencheurs. Elles peuvent également servir à rechercher les conséquences de défauts multiples identifiées. Des exemples de techniques descendantes sont l'Analyse par Arbre des Défaillances (ADD – voir CEI 61025) et l'Analyse par Arbre des Événements (AAE) ;

b) Les techniques ascendantes (inductives) conviennent pour rechercher les conséquences de défauts uniques identifiés. Des exemples de techniques ascendantes sont l'Analyse des Modes de Défaillance et de leurs Effets (AMDE – voir CEI 60812), Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC).

De plus amples informations sur les méthodes d'analyse sont données dans l'EN 1050:1996 (ISO 14121:1999), Annexe B.

5 Validation par essais

5.1 Généralités

Lorsque la validation par analyse ne suffit pas à démontrer la réalisation des fonctions de sécurité et des catégories spécifiées, des essais doivent être réalisés pour achever la validation. Les essais sont toujours complémentaires à l'analyse et sont souvent nécessaires.

Les essais de validation doivent être programmés et réalisés de façon logique. En particulier :

a) un plan des essais doit être présenté avant de commencer les essais et doit inclure :

   1) les spécifications d'essais ;

   2) les résultats d'essais attendus ;

   3) la chronologie des essais.

b) des rapports d'essais, comportant les éléments suivants, doivent être fournis :

   1) le nom de la personne qui a effectué l'essai ;

2) les conditions d'environnement (voir article 8) ;

3) les procédures d'essais et les équipements utilisés ;

4) les résultats d'essai.

c) les rapports d'essais doivent être comparés avec le plan des essais pour s'assurer que les objectifs de fonctionnement et de performances spécifiés sont atteints.

L'échantillon d'essai doit être utilisé dans des conditions aussi proches que possible de sa configuration opérationnelle définitive, c'est-à-dire avec tous les dispositifs périphériques et couvercles fixés.

Les essais peuvent être effectués manuellement ou automatiquement (par exemple par ordinateur).

Lorsqu'elle est pratiquée, la validation des fonctions de sécurité par essais doit être effectuée en introduisant des données d'entrée, combinées de diverses manières, dans les parties du système de commande relatives à la sécurité. Les données de sortie correspondantes doivent être comparées aux données de sortie spécifiées.

Il est recommandé d'appliquer systématiquement la combinaison de ces données d'entrée au système de commande et à la machine. Voici un exemple de cette logique : mise sous tension, mise en marche, fonctionnement, inversion de mouvement, remise en marche. Si nécessaire, une gamme étendue de données d'entrée doit être introduite pour prendre en compte les situations anormales ou inhabituelles et vérifier comment la partie du système de commande relative à la sécurité répond. Ces combinaisons de données d'entrée doivent prendre en compte tout dysfonctionnement prévisible.

Les objectifs de l'essai sont déterminés par les conditions d'environnement pour cet essai. Les conditions peuvent être :

— des conditions d'environnement pour l'utilisation prévues, ou

— des conditions spécifiques, ou

— une gamme donnée de conditions si une dérive est attendue.

NOTE Il convient que la plage de conditions considérée comme stable et dans laquelle les essais sont valides fasse l'objet d'un accord entre le concepteur et la(les) personne(s) responsable(s) de l'exécution des essais et soit inscrite dans le rapport.

5.2 Incertitude de mesure

L'incertitude des mesures au cours de la validation par essais doit être adaptée à l'essai effectué. En général, ces incertitudes de mesure doivent être effectuées à 5 K. pour les températures et à 5 % pour les mesures suivantes :

a) mesures de temps ;

b) mesures de pression ;

c) mesures de force ;

d) mesures électriques ;

e) mesures hygrométriques ;

f) mesures linéaires.

Les écarts par rapport à ces incertitudes de mesure doivent être justifiés.

5.3 Spécifications supérieures

Si, selon les informations contenues dans les documents d'accompagnement, le système de commande répond à des spécifications supérieures aux prescriptions de la présente norme, les spécifications supérieures doivent s'appliquer.

NOTE De telles spécifications supérieures peuvent s'appliquer si le système de commande doit résister à des conditions de fonctionnement particulièrement difficiles, par exemple : manipulation brutale, effets de l'humidité, hydrolyse, variations de la température ambiante, effets d'agents chimiques, corrosion, forte intensité de champs électromagnétiques, par exemple du fait de la proximité d'émetteurs.

5.4 Nombre d'échantillons d'essais

Sauf spécification contraire, les essais doivent être réalisés sur un seul échantillon de série de la (des) partie(s) relative(s) à la sécurité qui devrai(en)t résister à tous les essais correspondants.

La(les) partie(s) relative(s) à la sécurité soumis(es) aux essais ne doit (doivent) pas être modifiée(s) au cours des essais.

Certains essais peuvent modifier de manière permanente les performances de certains composants. Lorsque la modification permanente des composants place la(les) partie(s) relative(s) à la sécurité en dehors des limites de la spécification de conception, il peut être nécessaire d'utiliser un (de) nouvel (nouveaux) échantillon(s) pour les essais qui suivent.

Lorsqu'un essai particulier est destructif, et que des résultats équivalents peuvent être obtenus en procédant à des essais sur une partie isolée de l'équipement, un échantillon de cette partie peut être utilisé à la place d'un échantillon de l'équipement complet pour parvenir aux résultats de l'essai. Cette approche ne doit être appliquée que lorsqu'il a été établi par l'analyse que l'essai de la(des) partie(s) relative(s) à la sécurité est suffisant pour démontrer les performances de sécurité de l'équipement complet relatif à la sécurité.

6 Validation des fonctions de sécurité

Une étape importante est la validation des fonctions de sécurité assurées par les parties du système de commande relatives à la sécurité pour vérifier qu'elles répondent entièrement aux caractéristiques spécifiées. Dans le processus de validation, Il est important de rechercher les erreurs et particulièrement les omissions dans la spécification formulée qui est fournie avec le raisonnement de conception.

Le but de la validation des fonctions de sécurité est de s'assurer que les signaux de sortie relatifs à la sécurité sont corrects et dépendent logiquement des signaux d'entrée, conformément à la spécification. Il convient que la validation couvre toutes les conditions normales et anormales prévisibles par simulation statique et dynamique.

Les fonctions de sécurité spécifiées [conformément à l'EN 954-1:1996 (ISO 13849-1:1999) article 5] doivent être validées dans tous les modes de fonctionnement de la machine. Cela signifie que la validation doit être effectuée pour démontrer que la fonctionnalité est correcte :

— dans diverses configurations suffisantes pour s'assurer que toutes les sorties relatives à la sécurité sont réalisées sur l'ensemble de leur plage. Des essais (par exemple : de surcharge) peuvent être nécessaires pour valider les fonctions de sécurité spécifiées ;

— en réponse à des signaux anormaux prévisibles provenant d'une source d'entrée quelconque, y compris l'interruption et le rétablissement de l'alimentation en énergie.

NOTE Lorsque cela est approprié, il convient de considérer des combinaisons des différentes configurations.