NORME INTERNATIONALE

ISO 25119-3

Deuxième édition
2018-10

Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité —

Partie 3: Développement en série, matériels et logiciels

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —

Part 3: Series development, hardware and software

Numéro de référence
ISO 25119-3:2018(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

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 (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée 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. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.html.

Le présent document a été élaboré par le comité technique ISO/TC 23, *Tracteurs et matériels agricoles et forestiers,* sous-comité SC 19, *Électronique en agriculture*.

Cette deuxième édition annule et remplace la première édition (ISO 25199-3:2010), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— l'introduction a été modifiée pour ajouter des informations spécifiques sur les normes de sécurité;

— les conditions préalables à la sécurité fonctionnelle ont été spécifiées;

— l'Article 5 a été révisé pour:

  — spécifier les conditions préalables à la sécurité fonctionnelle, et

  — simplifier les exigences générales des concepts techniques de sécurité;

— des instructions supplémentaires ont été ajoutées dans l'ensemble du document pour vérifier la cohérence des spécifications et des rapports d'essai;

— l'Annexe B a été changée en une annexe normative;

— le présent document a fait l'objet d'une révision rédactionnelle.

Une liste de toutes les parties de la série ISO 25119 se trouve sur le site web de l'ISO.

Tout retour ou question sur le présent document doit être adressée à l'organisme national de normalisation de l'utilisateur. Une liste complète de ces organismes peut être consultée à l'adresse www.iso.org/members.html.

Introduction

L'ISO 25119 (toutes les parties) établit une approche pour l'évaluation, la conception et la vérification de toutes les activités relatives au cycle de vie de sécurité des parties relatives à la sécurité constituées de systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PES) utilisés sur les tracteurs agricoles et forestiers, sur les machines automotrices à conducteur porté et sur les machines portées, semi-portées et traînées utilisées en agriculture. Elle est également applicable aux équipements municipaux mobiles.

Le prérequis pour l'application de l'ISO 25119 (toutes les parties), est la réalisation d'une identification des risques et d'une analyse de risque (par exemple ISO 12100) adaptées pour la totalité de la machine. Il en résulte qu'un système E/E/PES est fréquemment prévu pour assurer des fonctions relatives à la sécurité, créant des *parties relatives à la sécurité des systèmes de commande* (SRP/CS). Ces parties peuvent être constituées de matériels et de logiciels, elles peuvent être des parties isolées du système de commande ou en faire partie intégrante, et elles peuvent soit assurer uniquement des fonctions relatives à la sécurité, soit faire partie d'une fonction opérationnelle.

En général, le concepteur (et, dans une certaine mesure, l'utilisateur) associe la conception et la validation de ces SRP/CS dans le cadre de l'appréciation du risque. L'objectif est de réduire le risque lié à un phénomène dangereux donné (ou à une situation dangereuse) dans toutes les conditions d'utilisation de la machine. Cela peut être réalisé en appliquant diverses mesures (aussi bien SRP/CS que non-SRP/CS) dans le but final de réaliser une condition de sécurité.

L'ISO 25119 (toutes les parties) aborde la capacité des parties relatives à la sécurité à réaliser une fonction relative à la sécurité dans des conditions prévisibles en cinq niveaux de performance. Le niveau de performance d'un canal contrôlé dépend de plusieurs facteurs, tels que la structure du système (catégorie), l'étendue du mécanisme de détection de défaut (couverture de diagnostic), la fiabilité des composants (temps moyen avant défaillance dangereuse, défaillances de cause commune), le processus de conception, la contrainte en service, les conditions environnementales et les procédures de fonctionnement. Trois types de défaillances sont susceptibles de provoquer des dysfonctionnements des systèmes E/E/PES conduisant à des situations potentiellement dangereuses sont considérés: les défaillances systématiques, les défaillances de cause commune et les défaillances aléatoires.

Afin de guider le concepteur pendant la conception, la vérification, et faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 (toutes les parties) définit une approche fondée sur une classification d'architecture avec différentes caractéristiques de conception et un comportement spécifique en cas de défaut.

Les niveaux et catégories de performance peuvent être appliqués aux systèmes de commande de tous les types de machines mobiles, des systèmes simples (par exemple valves auxiliaires) aux systèmes complexes (par exemple transmission par fil), ainsi qu'aux systèmes de commande d'équipements de protection (par exemple dispositifs de verrouillage ou dispositifs sensibles à la pression).

L'ISO 25119 (toutes les parties) adopte une approche fondée sur le risque pour déterminer les risques, tout en fournissant un moyen permettant de spécifier le niveau de performance requis pour les fonctions relatives à la sécurité à mettre en œuvre par les canaux E/E/PES relatifs à la sécurité. Elle fournit les exigences pour tout le cycle de vie de sécurité des E/E/PES (conception, validation, production, fonctionnement, maintenance, démantèlement) nécessaires pour assurer la sécurité fonctionnelle requise pour les E/E/PES liés aux niveaux de performance.

La hiérarchie des normes est la suivante:

a) Normes de type A (normes de sécurité fondamentales) précisant des notions fondamentales, des principes de conception et des aspects généraux valables pour tous les types de machines.

b) Normes de type B (normes de sécurité relatives à un groupe) traitant d'un aspect de la sécurité ou d'un type de dispositif conditionnant la sécurité valable pour une large gamme de machines:

   — normes de type B1 traitant d'aspects particuliers de la sécurité (par exemple, distances de sécurité, température de surface, bruit);

— normes de type B2 traitant de dispositifs conditionnant la sécurité (par exemple, commandes bi-manuelles, dispositifs de verrouillage, dispositifs sensibles à la pression, protecteurs).

c) Normes de type C (normes de sécurité par catégorie de machines) indiquant des prescriptions de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier.

Le présent document est une norme de type B1 tel que spécifié dans l'ISO 12100.

Le présent document concerne, en particulier, les groupes de parties prenantes suivants, représentant les acteurs du marché dans le domaine de la sécurité des machines:

— fabricants de machines (petites, moyennes et grandes entreprises);

— organismes de santé et de sécurité (autorités réglementaires, organismes de prévention des risques professionnels, surveillance du marché, etc.).

D'autres partenaires peuvent être concernés par le niveau de sécurité des machines atteint à l'aide du document par les groupes de parties prenantes mentionnés ci-dessus:

— utilisateurs de machines/employeurs (petites, moyennes et grandes entreprises);

— utilisateurs de machines/salariés (par exemple, syndicats de salariés, organisations représentant des personnes ayant des besoins particuliers);

— prestataires de services, par exemple sociétés de maintenance (petites, moyennes et grandes entreprises);

— consommateurs (dans le cas de machines destinées à être utilisées par des consommateurs).

Les groupes de parties prenantes mentionnées ci-dessus ont eu la possibilité de participer au processus d'élaboration du présent document.

De plus, le présent document est destiné aux organismes de normalisation élaborant des normes de type C.

Les exigences du présent document peuvent être complétées ou modifiées par une norme de type C.

Pour les machines qui sont couvertes par le domaine d'application d'une norme de type C et qui ont été conçues et fabriquées conformément aux exigences de cette norme, les exigences de la norme de type C prévalent.

Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité —

Partie 3:
Développement en série, matériels et logiciels

1 Domaine d'application

Le présent document établit des principes généraux pour la conception et le développement des parties relatives à la sécurité des systèmes de commande (SRP/CS) utilisés sur les tracteurs agricoles et forestiers, sur les machines automotrices à conducteur porté et sur les machines portées, semi-portées et traînées utilisées en agriculture. Elle peut être également applicable aux équipements municipaux mobiles (par exemple machines de nettoiement). Elle spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions de sécurité.

Le présent document n'est pas applicable aux:

— véhicules aéroportés et sur cousin d'air utilises en agriculture;

— équipements pour jardins et pelouses.

Le présent document spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions relatives à la sécurité. Il n'identifie pas de niveaux de performance pour des applications spécifiques.

NOTE 1 Les normes spécifiques à une machine donnée (normes de type C) peuvent spécifier des niveaux de performance (AgPL) pour des fonctions relatives à la sécurité dans des machines relevant de leur domaine d'application. Sinon, la spécification de l'AgPL est de la responsabilité du fabricant.

Le présent document est applicable aux parties relatives à la sécurité des systèmes électriques/électroniques/électroniques programmables (E/E/PES), dans la mesure où celles-ci sont liées aux systèmes mécatroniques. Elle couvre les éventuels phénomènes dangereux dus au comportement fonctionnel des systèmes E/E/PES liés à la sécurité, y compris les interactions entre ces systèmes. Elle ne traite pas des phénomènes dangereux dus à l'équipement lui-même (choc électrique, incendie, fumées, chaleur, rayonnement, toxicité inflammabilité, réactivité, corrosion, libération de l'énergie, et phénomènes dangereux similaires, à moins d'être causés directement par une défaillance du comportement des systèmes E/E/PES liés à la sécurité. Elle traite également de la défaillance du comportement des systèmes E/E/PES liés à la sécurité impliqués dans les mesures de protection, protecteurs ou fonctions liées à la sécurité en réponse aux phénomènes dangereux hors E/E/PES.

Exemples inclus dans le domaine d'application du présent document:

— Parties de machines relatives à la sécurité (SRP/CS) qui limitent le flux de courant dans les hybrides électriques pour empêcher les phénomènes dangereux de panne d'isolement/choc;

— interférence électromagnétique avec les SRP/CS;

— SRP/CS conçus pour empêcher les incendies.

Exemples non inclus dans le domaine d'application du présent document:

— panne d'isolement due aux frottements qui engendrent des phénomènes de chocs électriques;

— rayonnement électromagnétique nominal qui impacte les systèmes de commande environnants de la machine;

— corrosion engendrant une surchauffe des câbles électriques.

Le présent document n'est pas applicable aux systèmes non-E/E/PES (par exemple hydraulique, mécanique et pneumatique).

NOTE 2 Pour les principes de conception relatifs à la sécurité des machines, voir également l'ISO 12100.

Le présent document n'est pas applicable aux parties relatives à la sécurité des systèmes de commande fabriqués avant la date de sa publication.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 25119-1:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux pour la conception et le développement*

ISO 25119-2:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 2: Phase de projet*

ISO 25119-4:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 25119-1 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques pour l'utilisation en normalisation aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

4 Termes abrégés

Pour les besoins du présent document, les termes abrégés suivants s'appliquent.

AgPL	niveau de performance agricole (*agricultural performance level*)
$AgPL_r$	niveau de performance agricole requis (*required agricultural performance level*)
CAD	conception assistée par ordinateur (*computer-aided design*)
Cat	catégorie de matériel
CCF	défaillance de cause commune (*common-cause failure*)
DC	couverture de diagnostic (*diagnostic coverage*)
DC_{avg}	couverture moyenne de diagnostic (*average diagnostic coverage*)
UCE	unité de commande électronique
ETA	analyse par arbre d'événements (*event tree analysis*)

E/E/PES	systèmes électriques/électroniques/électroniques programmables *(electrical/electronic/programmable electronic systems*)
CEM	compatibilité électromagnétique
FMEA	analyse des modes de défaillance et de leurs effets
FSM	gestion de la sécurité fonctionnelle (*functional safety management*)
FTA	analyse par arbre de panne (*fault tree analysis*)
HARA	hazard analysis and risk assessment
HIL	matériel incorporé (*hardware in the loop*)
MTTF	temps moyen avant défaillance (*mean time to failure*)
$MTTF_D$	temps moyen avant défaillance dangereuse (*mean time to dangerous failure*)
$MTTF_{DC}$	temps moyen avant défaillance dangereuse pour chaque canal (*mean time to dangerous failure for each channel*)
PES	système électronique programmable (*programmable electronic system*)
QM	management (mesures) de la qualité (*quality measures*)
RAM	mémoire vive (*random-access memory*)
SOP	démarrage de la production (*start of production*)
SRL	niveau d'exigence du logiciel (*software requirement level*)
SRP	parties relatives à la sécurité (*safety-related parts*)
SRP/CS	parties relatives à la sécurité d'un système de commande (*safety-related parts of control systems*)
UML	langage de modélisation UML (*unified modelling language*)

5 Conception du système

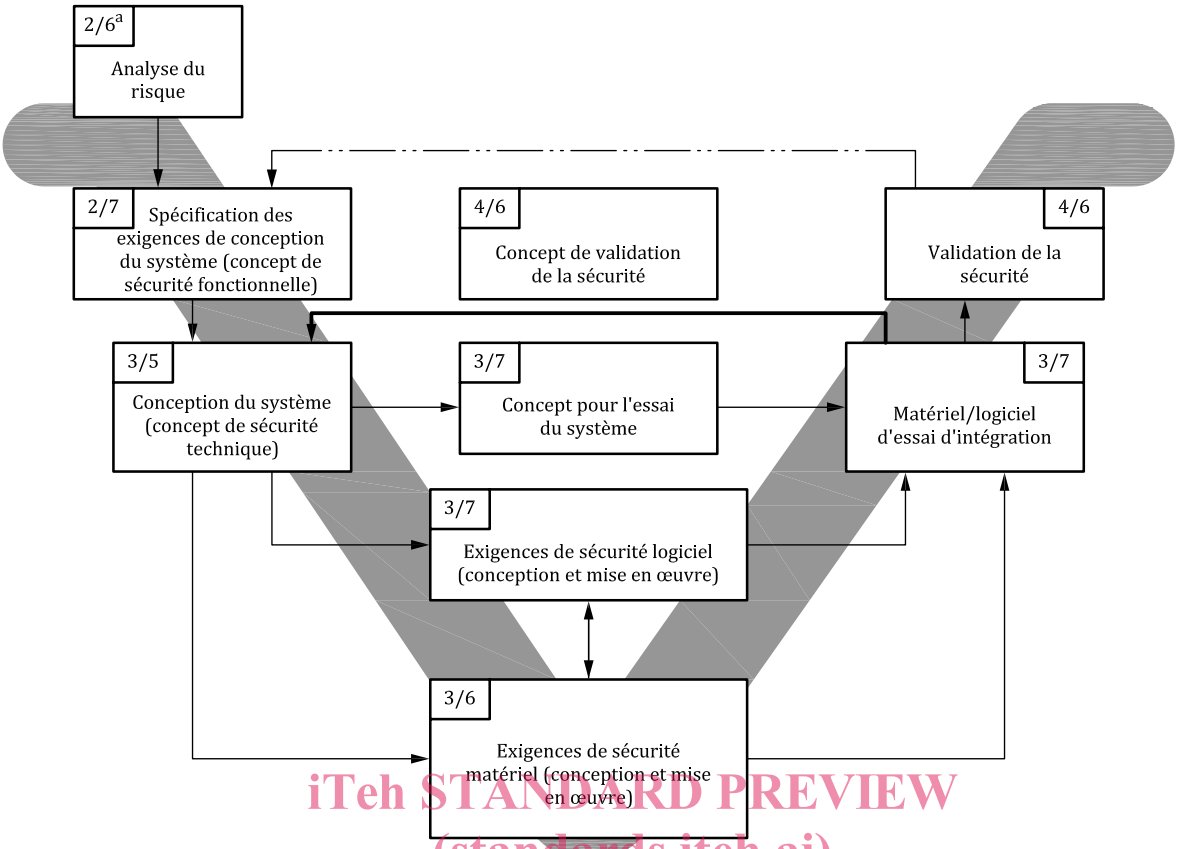
5.1 Objectifs

L'objectif est de définir une conception des systèmes pour la production d'une conception détaillée qui réponde aux exigences de sécurité pour tout le système relatif à la sécurité.

5.2 Généralités

Les exigences de sécurité constituent toutes les exigences visant à réaliser et à assurer la sécurité fonctionnelle. Pendant le cycle de vie de sécurité, les exigences de sécurité sont détaillées et spécifiées de manière plus approfondie par niveaux hiérarchiques. Les différents niveaux relatifs aux exigences de sécurité sont illustrés à la Figure 1. Pour la représentation globale de la procédure de développement des exigences de sécurité, voir également 5.4. Afin de prendre en charge la gestion des exigences de sécurité, il est recommandé d'utiliser des outils appropriés pour la gestion des exigences.

L'Annexe A fournit des lignes directrices pour un exemple de programme d'évaluation de la sécurité fonctionnelle associée à une AgPL = e.



Légende

→ résultat
← vérification
←··· validation

a Le premier chiffre correspond à la partie de l'ISO 25119, le deuxième, séparé par une barre oblique, à l'article de la partie c'est-à-dire, «2/6» signifie ISO 25119-2:2018, Article 6, «3/5» signifie ISO 25119-3:2018, Article 5, et ainsi de suite.

Figure 1 — Structuration des exigences de sécurité

5.3 Conditions préalables

Le concept de sécurité fonctionnelle (ISO 25119-2:2018, Article 7) est la condition préalable.

5.4 Exigences

5.4.1 Structuration des exigences de sécurité

Durant la phase de concept de sécurité fonctionnelle, les exigences de sécurité fonctionnelle sont spécifiées pour décrire le fonctionnement de base du système relatif à la sécurité avec lequel les objectifs de sécurité doivent être atteints. L'affectation de base des exigences de sécurité fonctionnelle à l'architecture du système est spécifiée par la spécification du concept de sécurité technique sous la forme d'exigences de sécurité technique. Cette architecture du système comprend aussi bien des matériels que des logiciels.

Les exigences de sécurité du matériel affinent et solidifient les exigences relatives à la sécurité technique. L'Article 6 décrit comment spécifier en détail les exigences du matériel.

Les exigences de sécurité du logiciel sont dérivées des exigences du concept de sécurité technique et du matériel sous-jacent. Les exigences relatives au logiciel définies dans l'Article 7 doivent être prises en compte.

Le présent article spécifie l'approche à suivre dans la spécification des exigences du concept de sécurité technique pendant la conception du système, fournissant ainsi une base pour la conception d'un système sans erreurs.

5.4.2 Concept de sécurité technique

5.4.2.1 Exigences générales du concept de sécurité fonctionnelle

Le document de concept de sécurité technique contient les exigences de sécurité technique pour le système.

Chaque exigence de sécurité technique doit être associée (par exemple, par référence croisée) à des exigences de sécurité de niveau supérieur qui peuvent être:

— d'autres exigences de sécurité technique;

— des exigences de sécurité fonctionnelle.

NOTE La traçabilité peut être grandement facilitée par l'utilisation d'outils de gestion d'exigence appropriés.

La mise en œuvre de chaque exigence de concept de sécurité doit considérer la faisabilité, le caractère non ambigu, la cohérence et l'exhaustivité.

Le concept de sécurité technique doit prendre en compte les éléments suivants:

a) tous les objectifs de sécurité et les exigences de sécurité fonctionnelle;

b) toutes les normes et réglementations statutaires pertinentes;

c) les résultats pertinents issus des outils d'analyse de sécurité (AMDE, FTA, etc.); l'analyse de sécurité fournit un support itératif pour le concept de sécurité technique pendant le développement du système.

L'exhaustivité du concept de sécurité technique augmente itérativement pendant la conception du système. Pour assurer l'exhaustivité:

1) la version du concept de sécurité technique et la version des sources sous-jacentes pertinentes doivent être spécifiées;

2) les exigences issues de la gestion des modifications (voir ISO 25119-4:2018, Article 11) doivent être satisfaites et, pour cette raison, les exigences de sécurité techniques doivent être structurées et formulées pour pouvoir prendre en charge un processus de modification;

3) les exigences de sécurité techniques doivent être revues (voir ISO 25119-4:2018, Article 6).

Le concept de sécurité technique doit considérer toutes les phases du cycle de vie (comprenant la production, l'opération du client, l'entretien courant et le démantèlement).

5.4.2.2 Spécification du concept de sécurité technique

5.4.2.2.1 Généralités

Le concept de sécurité technique doit comprendre les exigences de sécurité du matériel et du logiciel suffisantes pour la conception du SRP/CS, et doit être déterminé conformément à 5.4.2.1.

5.4.2.2.2 États et temps

Le comportement du SRP/CS, de ses composants ainsi que de leurs interfaces doivent être spécifiés pour tous les états de fonctionnement pertinents, y compris

— le démarrage,

— le fonctionnement normal,

— l'arrêt,

— le redémarrage après réinitialisation, et

— les états de fonctionnement inhabituels raisonnablement prévisibles (par exemple les états de fonctionnement dégradés).

En particulier, le comportement de défaillance et la réaction requise doivent être décrits avec exactitude. Des fonctions de fonctionnement d'urgence supplémentaires peuvent être incluses.

Le concept de sécurité technique doit spécifier un état de sécurité pour chaque exigence de sécurité fonctionnelle, la transition vers l'état de sécurité et la maintenance de l'état de sécurité. En particulier, il doit être spécifié si l'arrêt du SRP/CS représente immédiatement un état de sécurité, ou si un état de sécurité ne peut être atteint que par un arrêt contrôlé.

Le concept de sécurité technique doit spécifier, pour chaque exigence de sécurité fonctionnelle, le temps maximal susceptible de s'écouler entre l'occurrence d'une erreur et l'atteinte d'un état de sécurité (temps de réponse). Tous les temps de réponse pour les sous-systèmes et les sous-fonctions doivent être spécifiés dans le concept de sécurité technique.

Si aucun état de sécurité ne peut être atteint par un arrêt direct, un temps doit être défini pendant lequel une fonction spéciale de fonctionnement d'urgence doit être maintenue pour tous les sous-systèmes et sous-fonctions. Cette fonction de fonctionnement d'urgence doit être documentée dans le concept de sécurité technique.

5.4.2.2.3 Architecture, interfaces et conditions marginales de sécurité

L'architecture de sécurité et ses sous-composants doivent être décrits. En particulier, les mesures techniques doivent être spécifiées. Le concept de sécurité technique doit décrire séparément les composants suivants (le cas échéant):

— le système de détection, séparé pour chaque paramètre physique enregistré;

— diverses unités d'entrée et de sortie numériques et analogiques;

— le traitement, séparé pour chaque unité arithmétique/unité logique discrète;

— le système d'actionnement, séparé pour chaque actionneur;

— les afficheurs, séparés pour chaque unité d'indication;

— divers composants électromécaniques;

— la transmission de signal entre les composants;

— la transmission de signal à partir/en direction des systèmes externes au SRP/CS;

— l'alimentation.

Les interfaces situées entre les composants du SRP/CS, les interfaces d'autres systèmes et les fonctions dans la machine ainsi que les interfaces utilisateur doivent être spécifiées.

Les restrictions et conditions marginales du SRP/CS doivent être spécifiées. Cela s'applique en particulier aux valeurs externes pour toutes les conditions ambiantes dans toutes les phases du cycle de vie.

5.5 Produits fabriqués

Le produit fabriqué doit être applicable à la conception du système:

a) spécification du concept de sécurité technique.

6 Matériel

6.1 Objectifs

L'objectif est de définir les architectures de matériel acceptables pour les SRP/CS.

6.2 Généralités

L'amélioration de la structure du matériel des SRP/CS peut fournir des mesures permettant d'éviter, de détecter ou de tolérer les défauts. Les mesures pratiques peuvent inclure la redondance, la diversité et la surveillance.

En général, les critères de défaut suivants doivent être pris en compte.

— Si, en conséquence d'un défaut, des composants supplémentaires sont défectueux, le premier défaut et tous les défauts suivants sont considérés comme étant un seul défaut.

— Deux défauts isolés ou plus ayant une cause commune sont considérés comme étant un seul défaut (désigné *défaillance de cause commune*).

— L'occurrence simultanée de deux défauts indépendants est très improbable et, par conséquent, n'a pas besoin d'être prise en considération.

Des itérations entre le développement matériel et logiciel peuvent être requises pour réaliser les essais nécessaires de matériel.

6.3 Conditions préalables

La condition préalable est que les parties du concept de sécurité fonctionnelle soient réalisées par le matériel (ISO 25119-2:2018, Article 7).

La condition préalable pour l'intégration du système matériel et la validation de la sécurité matérielle montrée à la Figure 2 pour le matériel qui est commandé par un logiciel est le fonctionnement du logiciel lui-même.

6.4 Exigences

Le processus de développement du matériel doit commencer au niveau du système où les fonctions relatives à la sécurité et les exigences associées sont identifiées (voir Figure 2).

Le concept de sécurité fonctionnelle doit être utilisé pour identifier l'$AgPL_r$ pour chaque fonction relative à la sécurité du système (ISO 25119-2).

La sélection des catégories de matériel, $MTTF_{DC}$, DC et SRL doit être faite de sorte que l'AgPL résultante de l'individu ou de la combinaison SRP/CS satisfasse ou dépasse tous les $AgPL_r$ des exigences de sécurité fonctionnelle assignées.

Le système peut être subdivisé en sous-systèmes pour faciliter le développement.

Chaque phase du cycle de développement doit être vérifiée.

L'essai d'intégration du système matériel/logiciel montré à la Figure 1 doit être effectué en utilisant les composants matériels et logiciels préalablement soumis à l'essai.