NORME INTERNATIONALE

ISO 25119-3

Première édition
2010-06-01

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

Partie 3: Développement en série, matériels et logiciels

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

Part 3: Series development, hardware and software

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

Numéro de référence
ISO 25119-3:2010(F)

© ISO 2010

PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2010

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

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

Sommaire

Page

Avant-propos iv
Introduction v
1 Domaine d'application 1
2 Références normatives 1
3 Termes et définitions 1
4 Termes abrégés 2
5 Conception du système 3
5.1 Objectifs 3
5.2 Généralités 3
5.3 Conditions préalables 4
5.4 Exigences 4
6 Matériel 8
6.1 Objectifs 8
6.2 Généralités 8
6.3 Conditions préalables 8
6.4 Exigences 8
6.5 Catégories de matériel 10
6.6 Produits fabriqués 10
7 Logiciel 11
7.1 Planification de développement du logiciel 11
7.2 Spécification relative aux exigences de sécurité du logiciel 14
7.3 Architecture et conception du logiciel 18
7.4 Conception et mise en œuvre du module du logiciel 21
7.5 Essai du module du logiciel 30
7.6 Intégration et essai du logiciel 39
7.7 Validation de sécurité du logiciel 41
7.8 Paramétrage fondé sur le logiciel 44
Annexe A (informative) Exemple de programme relatif à une évaluation de la sécurité fonctionnelle au niveau AgPL = e 46
Annexe B (informative) Indépendance par partitionnement du logiciel 48
Bibliographie 57

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cee29771-5b5e-4107-8e9e-f14ec2768e2/iso-25119-3-2010

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

L'ISO 25119-3 a été élaborée par le comité technique ISO/TC 23, *Tracteurs et matériels agricoles et forestiers*, sous-comité SC 19, *Électronique en agriculture*.

L'ISO 25119 comprend les parties suivantes, présentées sous le titre général *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité*:

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

— *Partie 1: Principes généraux pour la conception et le développement*

— *Partie 2: Phase de projet*

— *Partie 3: Développement en série, matériels et logiciels*

— *Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien*

© ISO 2010 – Tous droits réservés

Introduction

L'ISO 25119 établit une approche pour la conception et l'évaluation de toutes les activités relatives au cycle de vie de sécurité des systèmes relatifs à la sécurité constitués de composants 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 remorquées utilisées en agriculture. Elle est également applicable aux équipements municipaux. Elle couvre les éventuels phénomènes dangereux dus au comportement fonctionnel des systèmes E/E/PES relatifs à la sécurité, indépendamment des phénomènes dangereux dus à l'équipement E/E/PES lui-même (par exemple choc électrique, incendie, niveau de performance nominal du E/E/PES dédié à la sécurité passive et active).

Les parties des systèmes de commande des machines concernées sont fréquemment prévues pour assurer les fonctions critiques 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 critiques, 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 de prévention (aussi bien SRP/CS que non-SRP/CS) dans le but final de réaliser une condition de sécurité.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

L'ISO 25119 aborde la capacité des parties relatives à la sécurité à réaliser une fonction critique 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 considérées: les défaillances systématiques, les défaillances de cause commune et les défaillances aléatoires.

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/eee20771-5b5e-4107-8e9e-f144ee276862/iso-25119-3-2010

Afin de guider le concepteur pendant la conception et faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 définit une approche fondée sur une classification de structures 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 adopte une approche fondée sur le risque du client pour déterminer les risques, tout en fournissant un moyen permettant de spécifier le niveau de performance cible 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.

© ISO 2010 – Tous droits réservés

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

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

La présente partie de l'ISO 25119 fournit des principes généraux pour le développement en série, les matériels et les logiciels 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 remorquées utilisées en agriculture. Elle peut être également applicable aux équipements municipaux (par exemple machines de balayage des rues). Elle spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions de sécurité.

La présente partie de l'ISO 25119 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 ne spécifie ni les fonctions de sécurité ni les catégories censées être utilisées dans un cas particulier.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-585e-4107-8e9e-f144ce276862/iso-25119-3-2010

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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 (y compris les éventuels amendements) s'applique.

ISO 25119-1:2010, *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 25119-2:2010, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 2: Phase de projet*

ISO 25119-4:2010, *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 données dans l'ISO 25119-1 s'appliquent.

© ISO 2010 – Tous droits réservés

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
EUC	équipement commandé (*equipment under control*)
AMDE	analyse des modes de défaillance et de leurs effets
AMDEC	analyse des modes de défaillance, de leurs effets et de leur criticité
EPROM	mémoire morte reprogrammable (*erasable programmable read-only memory*)
FSM	gestion de la sécurité fonctionnelle (*functional safety management*)
FTA	analyse par arbre de panne (*fault tree analysis*)
HAZOP	étude des phénomènes dangereux et de l'exploitabilité (*hazard and operability study*)
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*)
SRS	système relatif à la sécurité (*safety-related system*)
UML	langage de modélisation UML (*unified modelling language*)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

© ISO 2010 – Tous droits réservés

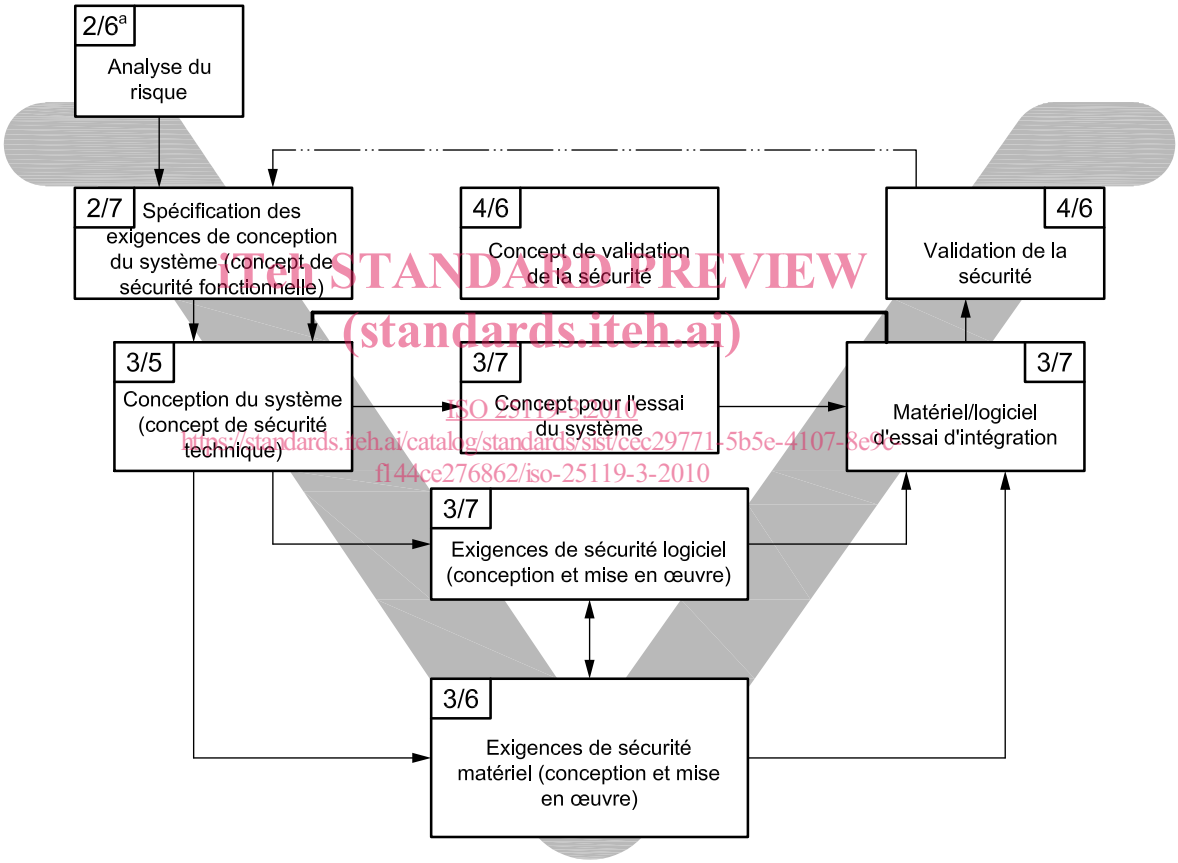
5 Conception du système

5.1 Objectifs

L'objectif est de définir un processus de développement pour la production d'une conception 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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9e-f144ce276862/iso-25119-3-2010

Légende

résultat

vérification

validation

[a] Dans l'ensemble de ces boîtes, le premier chiffre correspond à la partie de l'ISO 25119, le deuxième, séparé par une barre oblique, à l'article de la partie, par exemple, «2/6» signifie ISO 25119-2:2010, Article 6, «3/5» signifie ISO 25119-3:2010, Article 5, et ainsi de suite.

Figure 1 — Structuration des exigences de sécurité

© ISO 2010 – Tous droits réservés

5.3 Conditions préalables

Avant de commencer la conception du système, définir les exigences de la fonction relative à la sécurité, l'application et l'environnement de fonctionnement.

5.4 Exigences

5.4.1 Structuration des exigences de sécurité

Le concept de sécurité fonctionnelle spécifie 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 le 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 du concept de 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 pendant la conception du système, fournissant ainsi une base pour la conception d'un système sans erreurs.

5.4.2 Concept de sécurité fonctionnelle

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.4.2.1 Exigences générales du concept de sécurité fonctionnelle

Les fonctions de sécurité sont normalement identifiées pendant l'analyse de risque du système, et le document de concept de sécurité fonctionnelle contient les exigences de sécurité fonctionnelle pour le système.

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

La mise en œuvre de chaque exigence de concept de sécurité doit considérer les éléments suivants.

— **Faisabilité**

  En répertoriant les exigences de sécurité fonctionnelle, il faut veiller à la faisabilité de l'exigence en considérant les contraintes, telles que la technologie disponible, ainsi que les ressources financières et temporelles. Les personnes en charge de la mise en œuvre doivent comprendre et accepter les exigences de sécurité technique.

— **Caractère non ambigu**

  Les exigences de sécurité fonctionnelle doivent être formulées de façon aussi précise et non ambiguë que possible.

  NOTE Une exigence de sécurité fonctionnelle est formulée sans ambiguïté lorsqu'elle ne permet qu'une seule interprétation par les lecteurs prévus.

— **Cohérence**

  Les exigences de sécurité fonctionnelle ne doivent pas être autocontradictoires (cohérence interne) ni contredire d'autres exigences (cohérence externe).

  L'analyse des exigences et les comparaisons entre différentes exigences sont nécessaires pour assurer la cohérence externe. Il s'agit d'une tâche de gestion d'exigence.

— **Exhaustivité**

  Le concept de sécurité fonctionnelle doit prendre en compte toutes les normes et réglementations statutaires pertinentes.

© ISO 2010 – Tous droits réservés

Le concept de sécurité fonctionnelle doit prendre en compte tous les objectifs de sécurité pertinents issus de l'analyse de risque conformément à l'ISO 25119-2.

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

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

2) les exigences issues de la gestion des modifications (voir ISO 25119-4:2010, Article 10) doivent être satisfaites et, pour cette raison, les exigences de sécurité fonctionnelle doivent être structurées et formulées pour pouvoir prendre en charge un processus de modification;

3) les exigences de sécurité fonctionnelle doivent être revues (voir ISO 25119-4:2010, Article 6).

Le concept de sécurité fonctionnelle 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 fonctionnelle

Le présent article présente les informations qui sont censées être spécifiées dans le concept de sécurité fonctionnelle. Le concept de sécurité fonctionnelle peut être dérivé des scénarios de défaillance de la machine évalués pendant l'analyse du risque.

Chaque description de scénario de défaillance doit inclure les éléments suivants:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— conditions environnementales (déplacement sur une route verglacée, montée, descente, conditions météorologiques, etc.);

— conditions de la machine (moteur en marche, vitesse enclenchée, à l'arrêt, etc.);

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

— niveau AgPL qui en résulte;

— descriptions de l'état de sécurité (moteur arrêté, vanne arrêtée, transmission immobilisée, fonction continue à performance réduite, etc.).

5.4.3 Concept de sécurité technique

5.4.3.1 Exigences générales du concept de sécurité technique

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

Chaque concept de sécurité technique doit être associé (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, ou

— des buts et objectifs de sécurité.

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

De même que pour le concept de sécurité *fonctionnelle*, la mise en œuvre de chaque exigence de concept de sécurité doit considérer la faisabilité, le caractère non ambigu, la cohérence et l'exhaustivité.

© ISO 2010 – Tous droits réservés

— **Faisabilité**

En répertoriant les exigences de sécurité technique, il faut veiller à la faisabilité de l'exigence en considérant les contraintes, telles que la technologie disponible, ainsi que les ressources financières et temporelles. Les personnes en charge de la mise en œuvre doivent comprendre et accepter les exigences de sécurité technique.

— **Caractère non ambigu**

Les exigences de sécurité technique doivent être formulées de façon aussi précise et non ambiguë que possible.

NOTE Une exigence de sécurité technique est formulée sans ambiguïté lorsqu'elle ne permet qu'une seule interprétation par les lecteurs prévus.

— **Cohérence**

Les exigences de sécurité technique ne doivent pas être autocontradictoires (cohérence interne) ni contredire d'autres exigences (cohérence externe).

L'analyse des exigences et les comparaisons entre différentes exigences sont nécessaires pour assurer la cohérence externe. Il s'agit d'une tâche de gestion d'exigence.

— **Exhaustivité**

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

1) tous les objectifs de sécurité et les exigences de sécurité fonctionnelle,

2) toutes les normes et réglementations statutaires pertinentes,

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276b02/iso-25119-3-2010

3) 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:

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

5) les exigences issues de la gestion des modifications (voir ISO 25119-4:2010, Article 10) doivent être satisfaites et, pour cette raison, les exigences de sécurité technique doivent être structurées et formulées pour pouvoir prendre en charge un processus de modification;

6) les exigences de sécurité technique doivent être revues (voir ISO 25119-4:2010, 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).

5.4.3.2 Spécification du concept de sécurité technique

5.4.3.2.1 Généralités

Le concept de sécurité technique doit comprendre les exigences de sécurité du matériel et du logiciel suffisantes pour la conception de l'unité d'observation, et doit être déterminé conformément à 5.4.3.1.

 © ISO 2010 – Tous droits réservés

5.4.3.2.2 États et temps

Le comportement de l'unité d'observation et de ses modules ainsi que 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 de l'unité d'observation 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

5.4.3.2.3 Architecture, interfaces et conditions marginales de sécurité

L'architecture de sécurité et ses sous-modules doivent être décrits. En particulier, les mesures techniques doivent être spécifiées. Le concept de sécurité technique doit décrire séparément les modules 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 modules;

— la transmission de signal à partir/en direction des systèmes externes à l'unité d'observation;

— l'alimentation.

© ISO 2010 – Tous droits réservés

Les interfaces situées entre les modules de l'unité d'observation, les interfaces d'autres systèmes et les fonctions dans la machine ainsi que les interfaces utilisateur doivent être spécifiées.

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

6 Matériel

6.1 Objectifs

L'objectif est de définir les architectures de matériel acceptables pour les systèmes de commande relatifs à la sécurité.

6.2 Généralités

L'amélioration de la structure du matériel des parties relatives à la sécurité du système de commande 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 considérée comme étant très improbable.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

6.3 Conditions préalables

Les conditions préalables sont le niveau $AgPL_r$, déterminé pour chaque fonction de sécurité à réaliser par le matériel.

6.4 Exigences

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

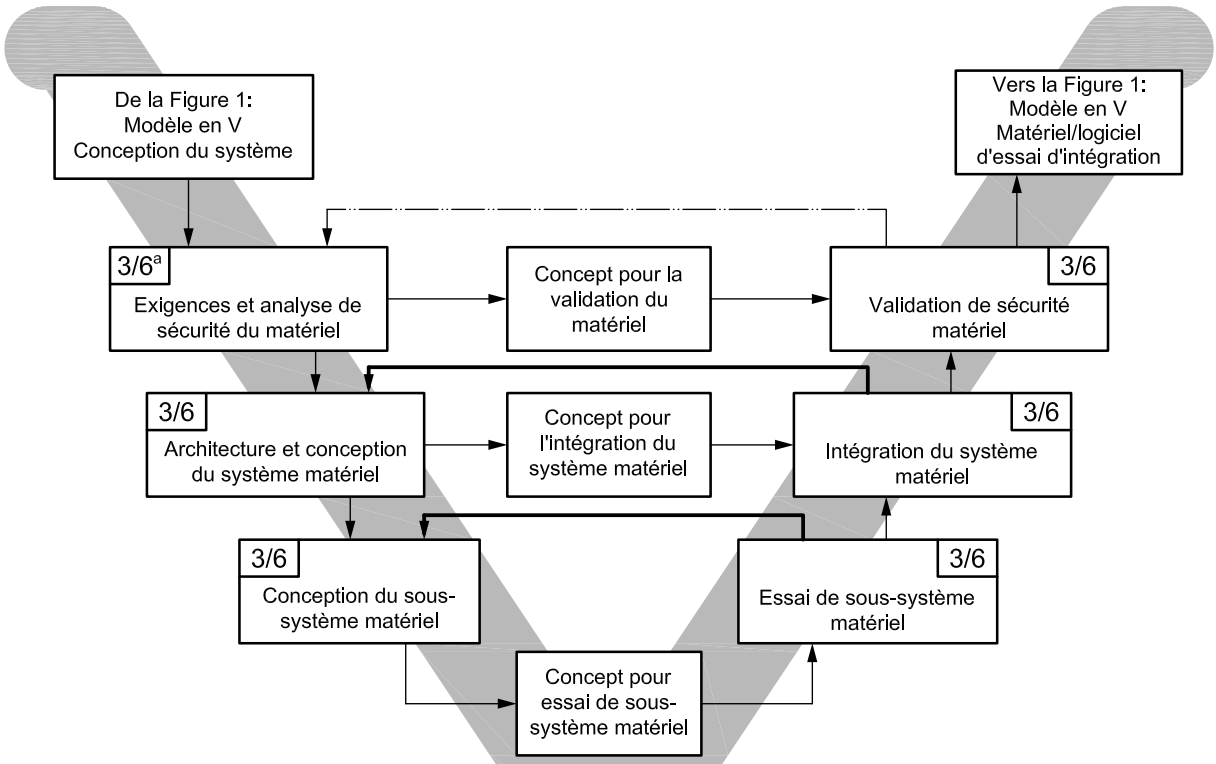
L'analyse de sécurité du matériel doit être utilisée pour identifier l'$AgPL_r$ pour chaque fonction de sécurité du système (voir l'ISO 25119-2).

Le concepteur doit grouper les fonctions dans des architectures appropriées (catégorie de matériel) avec les $MTTF_{dc}$, DC et CCF associés.

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

Chaque phase du cycle de développement doit être vérifiée.

© ISO 2010 – Tous droits réservés



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Légende

ISO 25119-3:2010
https://standards.iteh.ai/catalog/standards/sist/cec29771-5b5e-4107-8e9c-f144ce276862/iso-25119-3-2010

→ résultat

← vérification

← validation

[a] Le premier chiffre correspond à la présente partie de l'ISO 25119, le deuxième, séparé par une barre oblique, à l'Article 6.

Figure 2 — Développement de matériel — Modèle en V

La procédure de conception de l'architecture du système de matériel est la suivante.

a) Choisir une catégorie de matériel (ISO 25119-2:2010, Annexe A).

b) Identifier l'environnement de fonctionnement du composant et le niveau de contrainte.

c) Choisir les composants.

d) Calculer et vérifier que le $MTTF_{dC}$ atteint le niveau requis (ISO 25119-2:2010, Annexe B).

e) Déterminer et vérifier que la DC atteint le niveau requis (ISO 25119-2:2010, Annexe C).

f) Considérer la CCF (ISO 25119-2:2010, Annexe D).

g) Considérer les défaillances systématiques (ISO 25119-2:2010, Annexe E).

h) Considérer d'autres fonctions de sécurité (ISO 25119-2:2010, Annexe F).

NOTE L'itération peut être nécessaire pour les étapes ci-dessus.

© ISO 2010 – Tous droits réservés