NORME INTERNATIONALE

ISO 25119-2

Deuxième édition
2018-10

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

Partie 2: Phase de projet

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —
Part 2: Concept phase

Numéro de référence
ISO 25119-2:2018(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 25119-2:2010), qui a fait l'objet d'une révision technique.

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

— le Tableau 2 a été modifié pour spécifier des valeurs exactes;

— les Articles 6 et 7 ont été révisés;

— de nouveaux tableaux (Tableaux 4 et 5) ont été ajoutés pour indiquer des valeurs de DC et $MTTF_D$;

— la Figure 2 a été remplacée;

— les Annexes H et J, normatives, ont été ajoutées;

— l'Annexe I, informative, a été ajoutée;

— la rédaction du document a été révisée.

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

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

L'ISO 25119 (toutes ses parties) établit une approche pour l'évaluation, la conception et la vérification, pour toutes les activités relatives au cycle de vie de sécurité, des parties relatives à la sécurité comprenant les 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 ses 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 chargé d'assurer des fonctions relatives à la sécurité, créant des *parties de systèmes de commande relatives à la sécurité* (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 ses 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 défaillance susceptibles de provoquer des dysfonctionnements des systèmes E/E/PES conduisant à des situations potentiellement dangereuses sont considérés: la défaillance systématique, la défaillance de cause commune et la défaillance aléatoire.

Afin de guider le concepteur pendant la conception et la vérification, et de faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 (toutes ses 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 ses 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 structure des normes de sécurité dans le domaine des machines 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 génériques de sécurité) traitant d'un ou plusieurs aspects de la sécurité, ou d'un ou plusieurs types de protecteur 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 comme mentionné dans l'ISO 12100.

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

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

— les 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 pour la maintenance (petites, moyennes et grandes entreprises);

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

Les groupes de parties prenantes mentionnés ci-dessus ont eu la possibilité de participer à l'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 couvertes par le domaine d'application d'une norme de type C et qui ont été conçues et construites 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 2:
Phase de projet

1 Domaine d'application

Le présent document spécifie la phase de conception du 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. Il peut également s'appliquer aux équipements municipaux mobiles (par exemple machines de nettoiement).

Le présent document ne s'applique pas:

— aux véhicules aéroportés et sur coussin d'air utilisés en agriculture,

— aux équipements de jardinage ou horticoles.

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 s'applique 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. Il couvre les éventuels phénomènes dangereux dus au dysfonctionnement de systèmes E/E/PES relatifs à la sécurité, y compris l'interaction entre ces systèmes. Il ne traite pas des phénomènes dangereux associés aux événements suivants: choc électrique, incendie, fumées, chaleur, rayonnement, toxicité, inflammabilité, réactivité, corrosion, libération d'énergie et phénomènes dangereux similaires, à moins qu'ils ne soient causés directement par un dysfonctionnement des systèmes E/E/PES relatifs à la sécurité. Il couvre également le dysfonctionnement des systèmes E/E/PES relatifs à la sécurité qui sont impliqués dans les mesures de protection, protecteurs ou fonctions relatives à la sécurité en réponse aux phénomènes dangereux hors E/E/PES.

Exemples faisant partie du domaine d'application du présent document:

— SRP/CS limitant le flux de courant dans les hybrides électriques pour empêcher les phénomènes dangereux de panne d'isolement/choc;

— interférence électromagnétique avec les SRP/CS; et

— SRP/CS conçues pour empêcher les incendies.

Exemples ne faisant pas partie du domaine d'application:

— panne d'isolement due au frottement qui engendre 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 25119-3:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 3: Développement en série, matériels et logiciels*

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 donnés dans l'ISO 25119-1:2018 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables 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.

ADC	convertisseur analogique-numérique (*analogue to digital converter*)
AgPL	niveau de performance agricole (*agricultural performance level*)
$AgPL_r$	niveau de performance agricole requis (*required agricultural performance level*)
Cat	catégorie de matériel
CCF	défaillance de cause commune (*common-cause failure*)
CRC	contrôle de redondance cyclique
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
AMDE	analyse des modes de défaillance et de leurs effets
EPROM	mémoire morte reprogrammable (*erasable programmable read-only memory*)
FTA	analyse par arbre de panne (*fault tree analysis*)
HARA	analyse des phénomènes dangereux et appréciation du risque (*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	mesures de la qualité
RAM	mémoire vive (*random-access memory*)
SOP	démarrage de la production (*start of production*)
SRL	niveau d'exigence du logiciel (*software requirement level*)
SRP/CS	parties relatives à la sécurité d'un système de commande (*safety-related parts of control systems*)
UoO	unité d'observation

5 Concept — UoO

5.1 Objectifs

Cette phase a pour objectif de développer une compréhension adéquate de l'UoO afin de réaliser de manière satisfaisante toutes les tâches définies dans le cycle de vie de sécurité (voir ISO 25119-1:2018, Figure 2). Pour chaque UoO, une méthode appropriée doit être utilisée pour déterminer le niveau de performance requis. Les méthodes appropriées comprennent l'analyse du risque (décrite ci-dessous), d'autres normes, des exigences légales et l'expertise d'un organisme d'essai ou une combinaison de ceux-ci.

5.2 Conditions préalables

Les conditions préalables sont une description de la fonction relative à la sécurité à assurer par l'UoO, de ses interfaces, des exigences de sécurité et de fiabilité connues et du domaine d'application.

5.3 Exigences

5.3.1 Exigences fondamentales et conditions ambiantes

Les informations suivantes doivent être disponibles pour la fonction relative à la sécurité de l'UoO:

a) le domaine d'application, le contexte, l'objectif et les éléments connus;

b) les exigences fonctionnelles;

c) d'autres exigences et conditions ambiantes qu'il convient de prendre en compte, comprennant:

— les exigences techniques ou physiques, par exemple les conditions et les contraintes de fonctionnement, environnementales et environnantes;

— les exigences légales, notamment la législation, la réglementation, les normes (nationales et internationales) relatives à la sécurité;

d) les exigences historiques relatives à la sécurité et à la fiabilité, et le niveau de sécurité et de fiabilité atteint pour des UoO similaires ou apparentées.

5.3.2 Limites de l'UoO et ses interfaces avec d'autres UoO

Pour avoir une compréhension du fonctionnement de l'UoO dans son environnement, les informations suivantes doivent être prises en compte:

— les limites de l'UoO;

— ses interfaces et interactions avec d'autres UoO et composants;

— les exigences applicables aux fonctions relatives à la sécurité concernant les autres UoO.

5.3.3 Mise en correspondance et affectation des fonctions pertinentes aux UoO impliquées, sources de contrainte

Les sources de contrainte qui pourraient affecter la sécurité et la fiabilité de l'UoO doivent être déterminées. Cela comprend:

— l'interaction des différentes UoO;

— les contraintes de nature physique ou chimique (teneur en énergie, toxicité, explosivité, corrosivité, réactivité, combustibilité, etc.);

— d'autres événements externes (température, choc, CEM, etc.);

— les erreurs de fonctionnement humaines raisonnablement prévisibles; et

— les contraintes provenant de l'UoO et les événements déclenchant une défaillance (par exemple pendant l'assemblage ou la maintenance).

5.3.4 Déterminations supplémentaires

Outre les activités décrites en 5.3.2, les déterminations ou actions suivantes doivent être effectuées:

— déterminer si l'UoO est un nouveau développement ou une modification, une adaptation ou la dérivée d'une UoO existante, et, en cas de modification, réaliser une analyse d'impact pour régler le cycle de vie de sécurité en conséquence;

— préparer un plan et une spécification pour vérifier et valider les exigences relatives à l'UoO définie en 5.3.1;

— définir la gestion de projet pour les phases appropriées dans le cycle de vie;

— utiliser des données d'entrée adéquates relatives à l'évaluation de la fiabilité;

— utiliser des procédures, outils d'application et technologies adéquats;

— employer un personnel ayant la qualification appropriée.

5.4 Produits fabriqués

Les éventuels produits fabriqués de l'UoO doivent être:

a) des éléments inclus dans l'UoO;

b) la spécification des exigences fondamentales et des conditions ambiantes;

c) les limites de l'UoO et ses interfaces avec d'autres UoO;

d) les sources de contrainte;

e) des déterminations supplémentaires.

6 HARA: Détermination de l'AgPLr

6.1 Objectifs

Les objectifs principaux consistent à analyser les risques associés à une UoO défectueuse (une unité qui n'exécute pas les fonctions relatives à la sécurité comme prévu, telle que ne s'arrêtant pas convenablement, se déplaçant alors qu'elle est au point mort, direction active dans le mauvais sens), puis à attribuer un AgPLr approprié. Le risque est défini comme une combinaison de la probabilité d'un dommage et de la gravité de ce dommage (ISO 25119-1:2018, 3.39). Lors de la prise en compte de la probabilité d'apparition du dommage, si c'est approprié, la probabilité d'être exposé à une situation dangereuse avec une UoO défectueuse peut être prise en compte.

La procédure décrite en 6.2 à 6.4 fournit une méthodologie appropriée pour déterminer l'$AgPL_r$ à partir de l'analyse HARA.

6.2 Conditions préalables

La définition de l'UoO associée à chaque fonction relative à la sécurité.

6.3 Exigences

6.3.1 Procédures de préparation d'une analyse HARA

L'analyse HARA doit prendre en compte la totalité de la fonction relative à la sécurité, de manière à pouvoir fournir une spécification appropriée pour les SRP/CS. Si des décisions sont prises plus tard durant le cycle de vie de sécurité et si elles changent le domaine d'application, l'analyse HARA doit être revue en conséquence. Pour identifier les changements et leurs impacts sur les produits fabriqués, une analyse d'impact doit être effectuée conformément à l'ISO 25119-4:2018.

6.3.2 Les tâches d'une analyse HARA

Il doit être tenu compte des conditions opérationnelles dans lesquelles le dysfonctionnement de l'UoO conduira à des situations dangereuses, en cas d'utilisation correcte et en cas d'utilisation incorrecte raisonnablement prévisible.

6.3.3 Participants à l'analyse HARA

L'analyse HARA doit impliquer les personnes suffisantes pour s'assurer de disposer de l'ensemble de l'expertise pertinente.

NOTE Le fait d'impliquer des personnes de disciplines différentes constitue souvent un apport intéressant pour l'analyse HARA.

6.3.4 Classification d'un dommage potentiel

La gravité potentielle d'un dommage doit être déterminée et documentée.

Les effets potentiellement préjudiciables doivent être déduits en tenant compte de toutes les situations dangereuses résultant des dysfonctionnements de la fonction relative à la sécurité dans les conditions, les modes et les situations d'exploitation pertinents.

Une catégorisation doit être utilisée pour la description des dommages. Pour cette raison, la gravité du dommage est classée en quatre catégories: S0, S1, S2 et S3 (voir Tableau 1).

Les actions de l'opérateur de la machine impliquée et les tiers présents (par exemple les réparateurs, les autres opérateurs de machines, les autres usagers de la route, etc.) doivent être pris en compte et leur exposition au danger doit être documentée.

L'objectif de l'évaluation et la classification des dangers potentiels doivent être axés sur le danger pour les personnes et s'y limiter. Si l'analyse du dysfonctionnement de la fonction relative à la sécurité se limite clairement aux biens matériels et n'implique pas de danger pour les personnes, ce type de dysfonctionnement n'a pas besoin d'être classé comme étant relatif à la sécurité.

Aucune appréciation du risque approfondie n'est censée être effectuée pour les fonctions affectées à la classe de dommage S0.

Tableau 1 — Classification des blessures

S0	S1	S2	S3
Absence de blessures, dommages limités aux biens matériels	Blessures légères et modérées, nécessitant de consulter un médecin, rétablissement complet	Blessures graves et potentiellement mortelles (survie probable), perte partielle permanente de capacité de travail	Blessures potentiellement mortelles (survie incertaine), handicap grave

6.3.5 Classification de l'exposition dans la situation observée

Une analyse HARA doit tenir compte des effets d'exposition des dysfonctionnements possibles de la fonction relative à la sécurité dans toutes les conditions opérationnelles et conditions régionales de travail spécifiques correspondantes. Ces situations varient des activités de routine quotidiennes aux situations extrêmes rares. La variable «E» doit être utilisée pour catégoriser les différentes fréquences ou durées d'exposition. Cinq catégories, désignées E0, E1, E2, E3 et E4, sont utilisées (voir Tableau 2), où E est une estimation de la fréquence et de la durée d'exposition d'un opérateur ou d'un tiers à un phénomène dangereux lors duquel une défaillance est susceptible de mettre en danger l'opérateur ou le tiers. La méthode la plus appropriée pour chaque situation dangereuse, sa fréquence ou sa durée, doit être utilisée pour déterminer l'$AgPL_r$. S'il est déterminé que plusieurs catégories conviennent à une situation dangereuse particulière, c'est la méthode fournissant la catégorie la plus élevée qui doit être utilisée.

NOTE Un risque susceptible de produire une situation dangereuse peut résulter d'une combinaison d'états de la machine (par exemple de nature environnementale et/ou opérationnelle).

Tableau 2 — Classification de l'exposition à la situation dangereuse

Description	E0	E1	E2	E3	E4
Définition de la fréquence	Improbable (théoriquement possible, une fois pendant toute la durée de vie)	Événements rares (moins d'une fois par an)	Parfois (plus d'une fois par an)	Souvent (plus d'une fois par mois)	Fréquemment (presque à chaque mise en fonctionnement)
Définition de la durée $\frac{t_{exp}}{t_{av\,op}}$	Inférieure à 0,01 %	de 0,01 % à moins de 0,1 %	de 0,1 % à moins de 1 %	de 1 % à moins de 10 %	Supérieure ou égale à 10 %
t_{exp} durée d'exposition. $t_{av\,op}$ durée de fonctionnement moyen.					

6.3.6 Classification des possibilités d'éviter un dommage

L'évaluation des possibilités d'éviter un dommage implique de déterminer si un opérateur-type formé à la machine dispose d'un niveau de maîtrise de la situation dangereuse susceptible de se produire et s'il peut l'éviter, ou si la situation est totalement incontrôlable. De même, un tiers présent non formé peut disposer d'un niveau de maîtrise lui permettant d'éviter une situation dangereuse. La variable C doit être utilisée pour classer l'aptitude à éviter les situations dangereuses. La valeur de C pour une possibilité d'éviter les situations dangereuses ne doit tenir compte que de l'aptitude des personnes à éviter les situations dangereuses faisant suite au dysfonctionnement de la fonction relative à la sécurité et elle ne doit pas tenir compte de la fiabilité ni d'autres mesures prévues dans les SRP/CS et qui réduisent le risque en cas de dysfonctionnement. Les catégories utilisées (C0, C1, C2 et C3) représentent respectivement une catégorie «facilement contrôlable», «contrôlable», «généralement contrôlable» et «non contrôlable» (voir Tableau 3).

Tableau 3 — Classification des possibilités d'éviter un dommage

C0	C1	C2	C3
Facilement contrôlable L'opérateur ou le tiers présent contrôle la situation et le danger est évité.	Contrôlable Plus de 99 % des personnes contrôlent la situation. Dans plus de 99 % des occurrences, la situation ne débouche pas sur un cas dangereux.	Généralement contrôlable Plus de 90 % des personnes contrôlent la situation. Dans plus de 90 % des occurrences, la situation ne débouche pas sur un cas dangereux.	Aucune En général, l'opérateur-type formé ou le tiers présent ne parvient pas à éviter le danger.

6.3.7 Sélection de l'$AgPL_r$

La Figure 1 donne des indications pour déterminer l'$AgPL_r$ en associant les valeurs de gravité (S), d'exposition (E) et de contrôlabilité (C) pour chaque situation dangereuse identifiée.

NOTE L'expérience de l'utilisation en toute sécurité de la même machine ou d'une machine semblable et la compétence générale de sauvegarde des machines est nécessaire pour établir l'$AgPL_r$ en appliquant la Figure 1.

Les $AgPL_r$ sont désignés de AgP_L = a à AgP_L = e. Le niveau AgP_L = a présente les exigences du système les moins strictes, et AgP_L = e présente les exigences du système les plus élevées. Outre ces niveaux, il existe une désignation de mesure de la qualité, QM, qui exige implicitement un développement de système conformément à une norme reconnue de management de la qualité (par exemple ISO 9001). QM ne s'applique qu'aux fonctions pour lesquelles le risque est suffisamment faible pour permettre à la fonction d'être classée en tant que non relative à la sécurité au titre de l'ISO 25119 (toutes les parties).

Les phénomènes dangereux identifiés qui définissent les $AgPL_r$ liés à la fonction relative à la sécurité de l'UoO (voir 7.3.2) et leurs $AgPL_r$ associés doivent être décrits et documentés dans un rapport HARA.