Livre blanc

Tendances mondiales de la sécurité des machines

Nouvelles exigences pour PL et SIL

En savoir plus sur

Révisions à venir des normes EN ISO 13849 et CEI 62061

Impact sur le thème de la « cybersécurité »

Changements dans le domaine des « logiciels liés à la sécurité »

PHOENIX CONTACT

Introduction

Pour réagir rapidement et de manière flexible aux exigences des clients, il est indispensable d'avoir une production industrielle complexe et décentralisée. Dans ce contexte, le thème de la sécurité fonctionnelle gagne en importance. La tendance à la décentralisation comporte de nouveaux défis pour la protection des personnes, de l'environnement et des machines. Outre les dispositifs de sécurité classiques, tels que verrouillages de portes de protection, dispositifs d'arrêt d'urgence ou commutateurs de sécurité, on utilise de plus en plus, avec un degré de complexité croissant, des systèmes de sécurité programmables ou configurables pour sécuriser les machines et les installations.

En 2015, une tentative d unification entre les deux normes liées à la sécurité machines, ISO 13849 et CEI 62061, n a pas abouti. Aujourd'hui, les deux normes sont en cours de révision séparément. Pour la norme EN ISO 13849, une publication est prévue début 2023. L'expert en sécurité Carsten Gregorius, qui représente Phoenix Contact dans les comités de normalisation, explique quelles modifications sont à attendre en matière de PL et de SIL : sur certains points, comme dans le domaine des « logiciels liés à la sécurité » et le thème de la « cybersécurité », les deux normes se sont déjà rapprochées.

De nombreuses autres adaptations ont été intégrées, de sorte que l'on obtient globalement une continuité entre les deux normes. L'impact éventuel sur les évaluations de sécurité antérieures doit être évalué au cas par cas.

Vous trouverez ci-dessous des informations détaillées sur les modifications de la norme.

Sommaire

Qu'est-ce qui change pour PL et SIL ? 3
Définition du PLr nécessaire 6
Spécification de la fonction de sécurité 7
Composants éprouvés 8
Valeurs caractéristiques manquantes ? Valeurs de remplacement ! 8
Exigences relatives aux logiciels liés à la sécurité 10
Influence de la cybersécurité sur la sécurité fonctionnelle 12
Systèmes à faible demande pour les machines 12

Disgression : travaux au sein du comité de normalisation 13

Glossaire 16

Contact 17

1 Qu'est-ce qui change pour PL et SIL ?

La sécurité des machines et des installations pour la protection de l'utilisateur dépend essentiellement du respect de l'application des normes et des directives. En Europe, la base est représentée par la directive relative aux machines, qui soutient les entreprises par des prescriptions uniformes lors de la construction de machines axées sur la sécurité. Mais en dehors de l'Europe, de nombreuses normes de sécurité européennes ont un réel impact en raison de leur statut international. Dans ce contexte, les normes de sécurité fonctionnelle jouent également un rôle important. Les exigences relatives aux commandes de machines sont définies aussi bien dans la norme EN ISO 13849 que dans la norme CEI 62061.

Outre le souci fondamental d'améliorer la lisibilité des normes, les axes de travail sur la norme EN ISO 13849 ont porté, entre autres, sur la spécification claire des exigences de sécurité (SRS). En outre, la détermination du niveau de risque PLr, pour lequel il existe des spécifications détaillées pour la détermination du paramètre P, est étendue. Les exigences relatives aux logiciels liés à la sécurité sont notamment concrétisées.

Présentation des principaux changements dans les normes EN ISO 13849 et CEI 62061

EN ISO 13849	CEI 62061
Définitions étendues pour la détermination du paramètre P (niveau de risque PLr)	Changement de la désignation de « SILCL » à « SIL »*
Spécification univoque des exigences de sécurité (SRS)	Prise en compte des applications à faible demande (pas encore prises en compte dans la version de la norme de 2021, à venir dans un amendement ultérieur)
Définition concrète des « éléments de construction éprouvés »	Adaptation du processus de validation sur la base de EN ISO 13849*
Adaptation du processus de validation sur la base de la norme EN ISO 13849-2*	
Valeurs de remplacement PFH_D pour les entrées et les sorties	Le champ d'application devient indépendant de la technologie (ne se limite plus à l'E/E/PES)*
Exigences concrètes pour les logiciels liés à la sécurité	
Influence de la cybersécurité sur la « sécurité fonctionnelle »	
Définition concrète de la « couverture de diagnostic » (DC)*	Exemples de taux d'erreur ($MTTF_D$), de taux de couverture de diagnostic (DC) selon la norme EN ISO 13849*
Détails du « défaut de cause commune » (Common Cause Failure) en ce qui concerne l'influence de la CEM*	Exemples d'évaluation des défauts de cause commune selon la norme EN ISO 13849*
Types d'appareil 1 à 4 (annexe O)*	

D'autres modifications concernent, pour la norme EN ISO 13849, des concrétisations relatives à

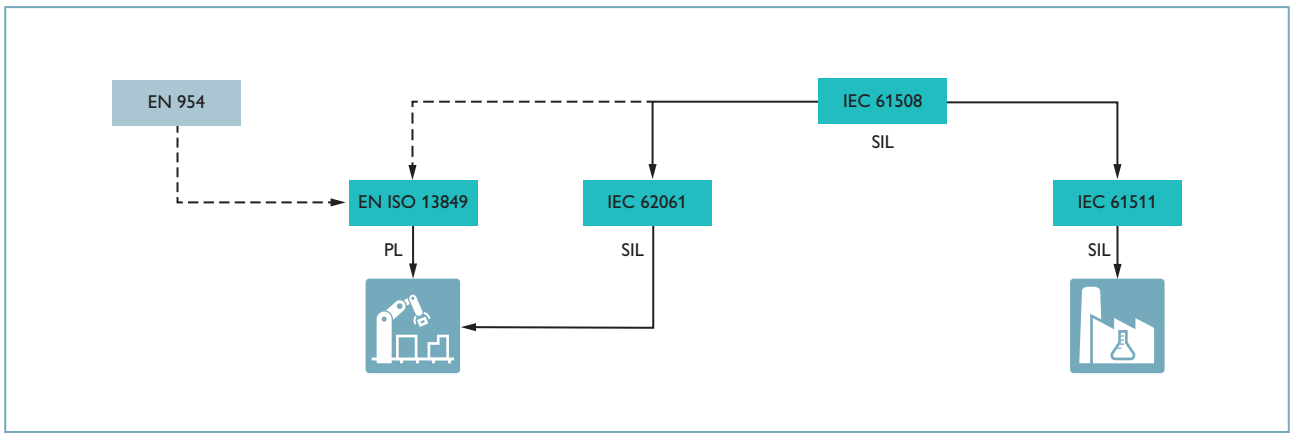
* Les détails ne seront pas traités dans le livre blanc

la couverture du diagnostic (DC) ainsi qu'à la définition des « composants éprouvés ». L'aspect des « défaillances de cause commune » (« Common Cause Failure ») a été détaillé dans la norme EN ISO 13849 en ce qui concerne l'influence de la CEM.

Pour des raisons de cohérence avec la CEI 61508 et d'autres normes sectorielles, la CEI 62061 a subi une adaptation importante au niveau des grandeurs caractéristiques en matière de technique de sécurité : à l'avenir, la notion de « SILCL » (clause SIL) sera remplacée par celle de « SIL ». En outre, des détails sont fournis sur la détermination des taux de défauts des composants ainsi que sur le processus de validation. Lors de la définition des taux de défaillance des composants selon la norme CEI 62061, un lien a été établi entre le terme utilisé λ_D et les définitions $MTTF_D$[1] et $B10_D$[2] utilisées dans la norme EN ISO 13849. La validation des fonctions de sécurité doit montrer que les exigences relatives aux éléments de commande de sécurité sont réalisées conformément à leurs caractéristiques spécifiées. La nouveauté de la norme CEI 62061 est l'organigramme du processus de validation, connu de la partie 2 de la norme EN ISO 13849.

Enfin, les deux normes abordent l'influence de la cybersécurité sur la « sécurité fonctionnelle ».

Les exigences relatives aux commandes de machines sont définies à la fois dans la norme



Signification des normes EN ISO 13849 et CEI 62061

EN ISO 13849 et dans la norme CEI 62061. De nombreuses normes C font référence à au moins une des deux normes pour la conception sécurisée des machines. Les deux normes prennent en compte des aspects de la norme de base CEI 61508. La norme EN ISO 13849 a été créée il y a environ 20 ans à partir de l'ancienne norme EN 954, alors que la norme CEI 62061 a été développée en tant que norme sectorielle pour les « machines ».

Parallèlement, il existe la norme sectorielle CEI 61511 pour l'industrie des process.

[1] $MTTF_D$: temps moyen jusqu'à la prochaine défaillance dangereuse

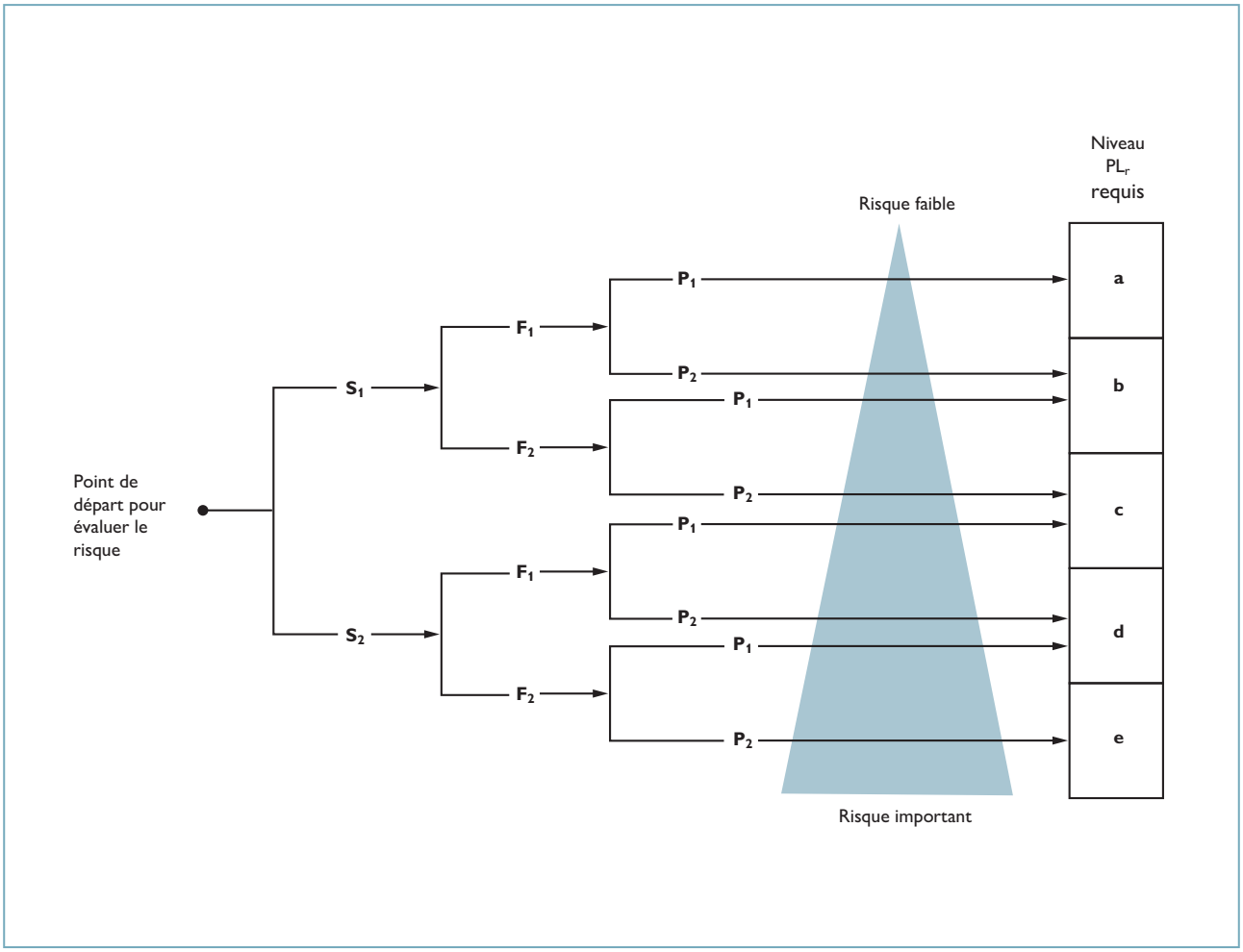
[2] $B10_D$: nombre moyen de cycles de commutation jusqu'à ce que 10 % des composants soient dangereusement défaillants

Définition du PLr nécessaire selon EN ISO 13849

Le « niveau de performance requis (PLr) » revêt une importance centrale dans le processus de réduction des risques. Selon le niveau de risque, l'un des cinq niveaux « a » à « e » est choisi en fonction des paramètres suivants : S (ampleur des dommages), F (fréquence d'exposition au danger) ou P (possibilité d'éviter le danger).

Par le passé, la question s'est posée, notamment pour le paramètre P, de savoir quand il fallait choisir P1 (possible, sous certaines conditions) ou P2 (impossible).

Pour déterminer le paramètre P1 ou P2, une aide à la sélection, qui évaluera les aspects de qualification, de vitesse de propagation du danger ainsi que de complexité, sera mise à disposition à l'avenir.



Détermination du PLr

Aide à la sélection pour déterminer le paramètre P

Description	A	B	C
Formation	Personnel formé	Personnel non formé	–
Vitesse du mouvement dangereux	Faible : p. ex. <250 mm/s, temps pour atteindre le danger >3 s	Moyen : p. ex. 251 mm/s - 1 000 mm/s, temps pour atteindre le danger <3 s	Élevé : p. ex. <1 000 mm/s, temps pour atteindre le danger <1 s
Possibilité géographique de se soustraire au danger	> = 50 % des cas	< 50 % des cas	Impossible
Possibilité de reconnaissance	> = 50 % des cas	< 50 % des cas	Impossible
Complexité (nombre/temps d'interventions de l'opérateur)	Faible degré de complexité (p. ex. réglage des pinces de serrage, mise en place des pièces à usiner)	Degré de complexité élevé ou moyen (recherche d'erreurs, réglage en mode par impulsions)	–

En fonction du nombre de classifications A, B ou C qui en résultent, il est alors possible de définir le paramètre P1 ou P2. Si le processus d'évaluation définit au moins 1 x C ou 3 x B, cela conduit directement à une classification P2.

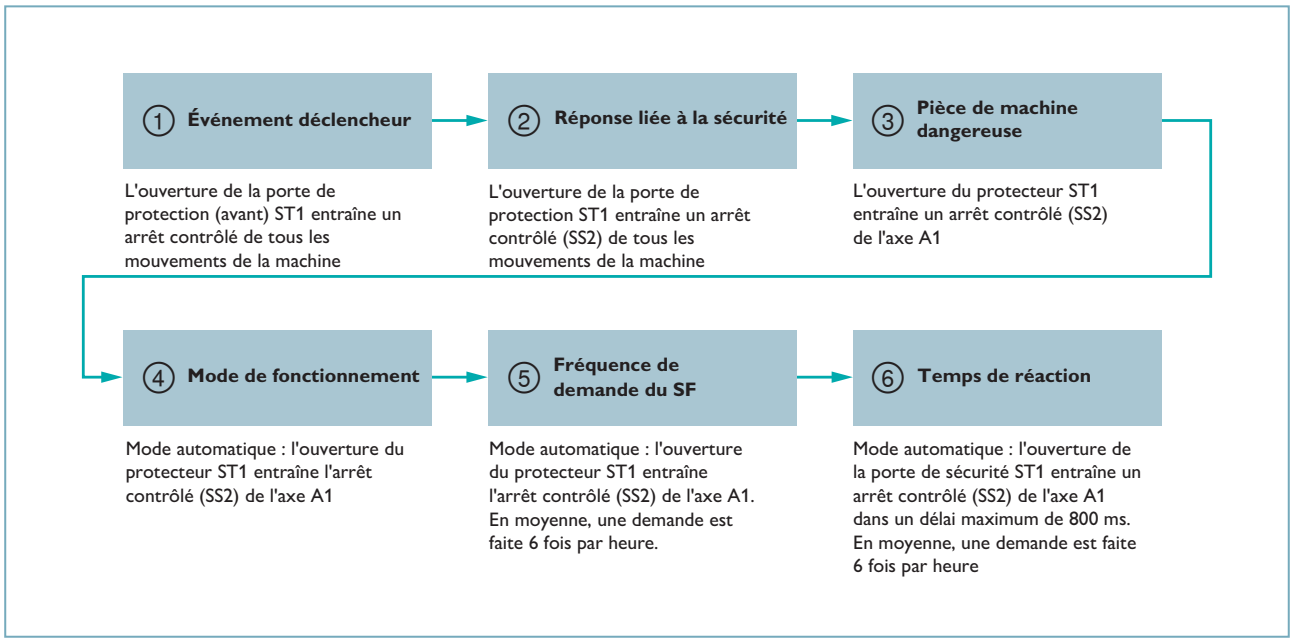
Spécification de la fonction de sécurité selon EN ISO 13849

Les incidents critiques sur les automates relatifs à la sécurité sont souvent dus à une spécification insuffisante. Cela peut conduire à ce que, malgré toutes les autres étapes de vérification correctement effectuées, seule une réduction insuffisante des risques soit finalement atteinte.

C'est pourquoi les rédacteurs de la norme EN ISO 13849 ont mis l'accent sur la description détaillée de ce que l'on appelle les SRS (Safety Requirements Specification).

Les questions suivantes doivent soutenir le processus de validation :

1. Quel est l'événement déclencheur ?
2. Qu'est-ce que la réaction axée sur la sécurité ?
3. Quelles sont les parties de la machine qui présentent un danger ?
4. Dans quel mode de fonctionnement la fonction de sécurité agit-elle ?
5. À quelle fréquence la fonction de sécurité est-elle sollicitée ?
6. Dans quel temps de réponse l'état sûr est-il atteint ?



Exemple de spécification d'une fonction de sécurité

L'exemple montre, les différentes étapes nécessaires à une « spécification des exigences de sécurité » détaillée. Cette approche permet d'utiliser des outils largement répandus qui prennent également en charge cette approche (par exemple SISTEMA[3]).

Composants éprouvés selon EN ISO 13849

La notion de « composants éprouvés » est particulièrement pertinente pour la conception selon la catégorie 1 de la norme EN ISO 13849. Sont considérés comme « éprouvés » les composants qui ont déjà été utilisés avec succès et documentés dans des applications similaires par le passé. Alternativement, sont considérés comme éprouvés les composants qui ont été fabriqués et vérifiés quant à leur aptitude et à leur fiabilité pour des applications liées à la sécurité. Un composant est accepté comme « éprouvé » en fonction de l'application, par exemple en raison des influences environnementales. Les composants électroniques complexes (p. ex. API, microprocesseur, circuit intégré spécifique à l'application) ne sont pas considérés comme équivalents.

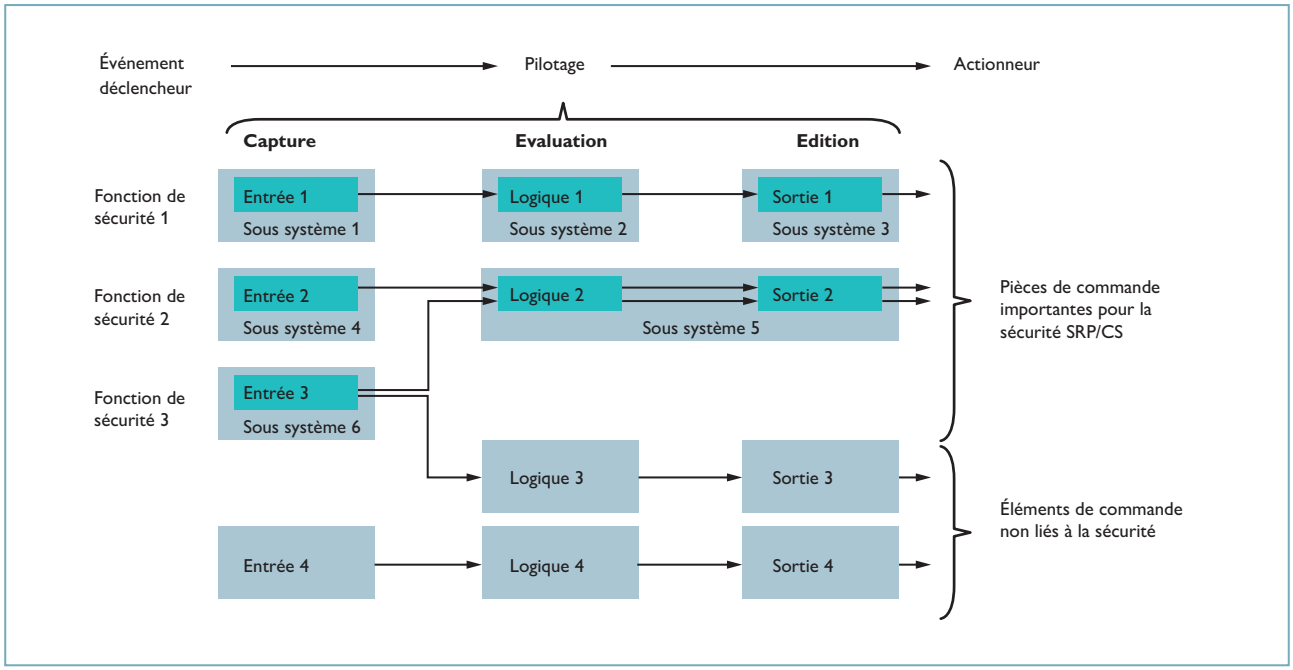
Valeurs caractéristiques manquantes ? Valeurs de remplacement selon EN ISO 13849

Après la définition de la fonction de sécurité (SRS) et la détermination du PLr selon EN ISO 13849, les parties de la commande relatives à la sécurité sont d'abord identifiées, puis la fonction de sécurité est décomposée en « sous-systèmes ». Dans ce contexte, les sous-systèmes peuvent être affectés à différentes fonctions de sécurité.

[3] SISTEMA : sécurité des systèmes de commande sur les machines
(éd. IFA = Institut pour la santé et la sécurité au travail de l'assurance-accidents légale allemande)

Les valeurs caractéristiques en matière de technique de sécurité (PFH_D, durée d'utilisation, etc.) sont ensuite déterminées pour chaque sous-système. Dans le cas le plus simple, l'utilisateur se sert des valeurs mises à disposition par le fabricant du composant (par exemple l'API de sécurité). Cependant, des composants standard pour lesquels ces valeurs caractéristiques ne sont pas disponibles sont utilisés dans certaines applications.

Jusqu'à présent, on pouvait partir d'un $MTTF_D$ = dix ans. Une hypothèse qui est toutefois trop « conservatrice » dans de nombreux cas. À l'avenir, il sera possible de travailler avec les valeurs de remplacement PFH_D du tableau ci-dessous pour les sous-systèmes dotés de composants discrets, si aucune donnée du fabricant n'est disponible.



Fonctions de sécurité et affectation aux sous-systèmes

	PFHD 1/h	Catégorie B	Catégorie 1	Catégorie 2	Catégorie 3	Catégorie 4
PL b	$5*10^{-6}$	X	O	O	O	O
PL c	$1,7*10^{-6}$	–	X*	X*	O	O
PL d	$2,9*10^{-7}$	–			X*	O
PL e	$4,7*10^{-8}$	–	–	–	–	X*

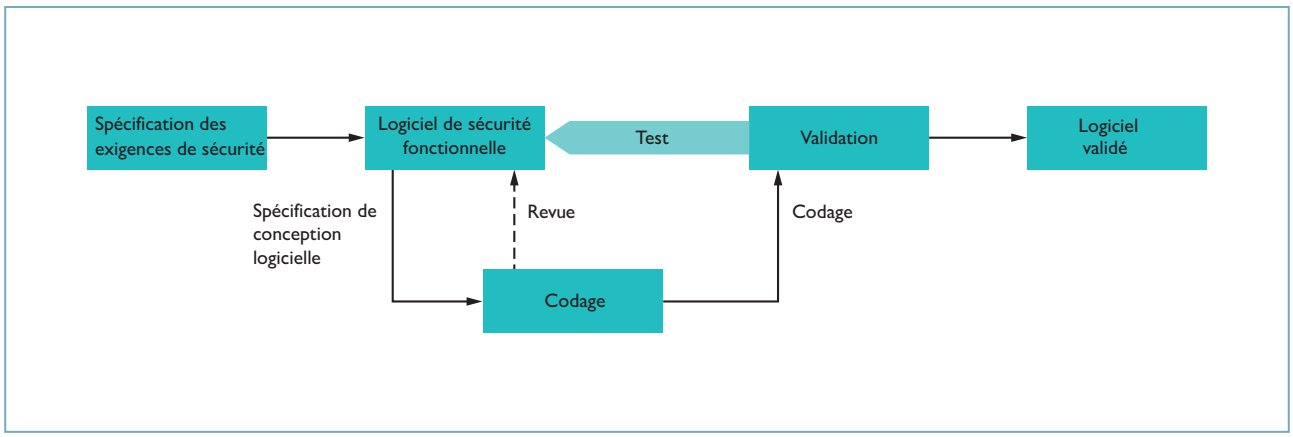
Valeurs de remplacement PFH_D pour les entrées et les sorties

X : la catégorie appliquée est recommandée. O : la catégorie appliquée est facultative
* les composants éprouvés et les principes éprouvés en matière de sécurité doivent être utilisés
-: la catégorie n'est pas autorisée

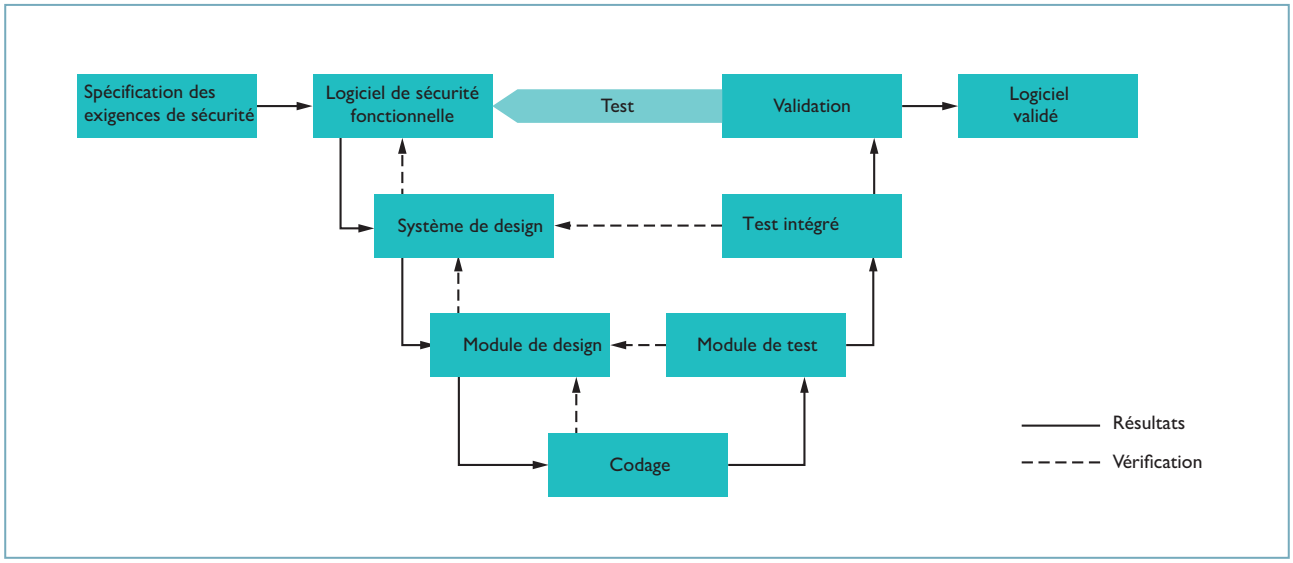
Exigences relatives aux logiciels liés à la sécurité selon EN ISO 13849 / CEI 62061

Les systèmes configurables ou programmables, déjà certifiés selon la norme CEI 61508, sont de plus en plus utilisés pour les commandes de machines.

En particulier pour les systèmes cités précédemment ainsi que pour les systèmes utilisant les langages LVL[4], on peut s'attendre à l'avenir à des simplifications importantes lors de la vérification et de la validation des fonctions de sécurité. Ainsi, le modèle V existant dans la norme EN ISO 13849 est simplifié pour ce cas d'application, de sorte qu'il ne reste que les étapes « codage » et « test logiciel » en plus de la SRS logicielle.



Modèle V simplifié



Modèle V pour les langages FVL[5]

[4] LVL : Limited Variability Languages = langages de programmation avec une étendue de langage limitée

Toutefois, si des langages FVL[5] tels que Ada, C, Assembler, etc. sont utilisés, le modèle V actuel reste obligatoire dans l'application.

Par analogie, la norme CEI 62061 définit des « niveaux logiciels ». Trois niveaux sont décrits dans la norme : la première étape décrit les systèmes préconçus (« pre-designed ») avec des langages LVL, pour lesquels une procédure de validation simplifiée est possible (comme dans la norme EN ISO 13849). Lors de l'utilisation de langages dits de programmation étendue, le processus de vérification et de validation semble plus étendu.

Le tableau ci-dessous indique les degrés d'indépendance minimaux requis qui en résultent pour le logiciel de niveau 1. De plus, l'utilisateur peut utiliser le modèle V simplifié (voir EN ISO 13849).

En résumé, l'utilisation de systèmes et de blocs logiciels pré-certifiés permet d'espérer une simplification considérable du processus de vérification et de validation.

Niveau logiciel	**Plateforme** (combinaison de matériel et de logiciels)	**Exemple**
1	« Pre-designed » selon la norme CEI 61508 (logiciel d'application qui utilise LVL)	API de sécurité avec LVL ou module de sécurité programmable
2	« Pre-designed » selon la norme CEI 61508 (logiciel d'application qui n'utilise pas de LVL)	API de sécurité avec le langage de programmation étendue selon CEI 62061
3	« Pre-designed » selon la norme CEI 61508 (logiciel d'application qui n'utilise pas de LVL)	API de sécurité avec LVL ou langage de programmation étendue selon CEI 61508

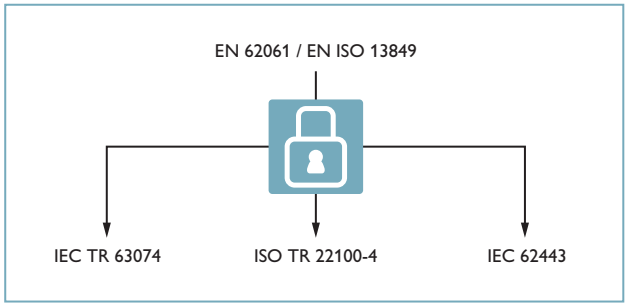
Degré d'indépendance minimal	**SIL requis pour la fonction de sécurité**		
	1	**2**	**3**
Même personne	Insuffisant	Insuffisant	Insuffisant
Autre personne	Uniquement si des modules logiciels pré-certifiés sont utilisés	Uniquement si des modules logiciels pré-certifiés sont utilisés	Insuffisant
Personne indépendante*	Suffisant	Suffisant	Suffisant

* En fonction de l'organisation de l'entreprise et de l'expertise au sein de l'entreprise, l'exigence d'une « personne indépendante » peut devoir être satisfaite par le recours à une organisation externe. Les entreprises qui disposent d'organisations internes compétentes en matière d'évaluation des risques et d'application de systèmes de sécurité peuvent utiliser leurs propres ressources pour satisfaire aux exigences d'une organisation indépendante, à condition que celles-ci soient indépendantes et séparées, par la direction et d'autres ressources, de celles qui sont responsables du développement principal.

[5] FVL : Full Variability Languages = langages de programmation étendue

Influence de la cybersécurité sur la sécurité fonctionnelle selon EN ISO 13849/CEI 62061

Contrairement à la sécurité fonctionnelle, la cybersécurité protège les biens contre toute dégradation préjudiciable due à des attaques intentionnelles ou accidentelles concernant la disponibilité, l'intégrité et la confidentialité des données. Des mesures préventives, techniques et organisationnelles sont utilisées à cet effet.



Situation normative :
cybersécurité pour la sécurité fonctionnelle

La mise en réseau croissante des systèmes d'automatisation permet toutefois de laisser apparaître des scénarios qui requièrent une nouvelle approche, en particulier des applications de sécurité. Les interfaces réseau entre l'informatique de bureau et le réseau de production constituent une porte d'entrée importante pour les cybercriminels. Ce danger potentiel se reflète également dans les deux projets de normalisation et doit être pris en compte à l'avenir, par exemple en réalisant une évaluation des risques informatiques sur le modèle de la norme CEI 62443.

Systèmes à faible demande pour les machines selon la norme CEI 62061

D'une part, le champ d'application de la directive relative aux machines est très large dans l'application pratique. Outre les machines classiques, des installations telles que les turbines à gaz et à vapeur, les compresseurs, les générateurs ou les pompes sont ainsi également concernées par la directive. D'autre part, les deux normes harmonisées relatives à la sécurité fonctionnelle – EN ISO 13849 et CEI 62061 – « Applications à faible demande »[6] ne sont pas encore prises en compte. Par la suite, l'absence de présomption de conformité a créé une insécurité juridique pour les fabricants de tels systèmes. La CEI 62061 reprendra a minima cette approche dans un amendement futur, en définissant désormais des valeurs limites de défaillance PFD[7] sur le modèle de la CEI 61508.

Par conséquent, si la CEI 62061 est correctement appliquée, les applications à faible demande peuvent désormais être évaluées en utilisant la « présomption de conformité » dans le champ d'application de la directive relative aux machines.

SIL	Valeurs limites de probabilité moyenne d'une défaillance dangereuse sur sollicitation à faible demande
1	$< 10^{-1}$
2	$< 10^{-2}$
3	$< 10^{-3}$

[6] Mode de fonctionnement dans lequel la fréquence des demandes d'une fonction de sécurité n'est pas supérieure à 1 par an et n'excède pas le double de la fréquence des tests de fonctionnement

[7] Probability of dangerous failure on demand

2 Disgression : travaux au sein du comité de normalisation

Les expertes et experts de Phoenix Contact sont représentés dans tous les comités de normalisation importants. En tant qu'expert en sécurité, Carsten Gregorius représente Phoenix Contact dans les comités nationaux de normalisation pour les normes EN ISO 13849 et CEI 62061.

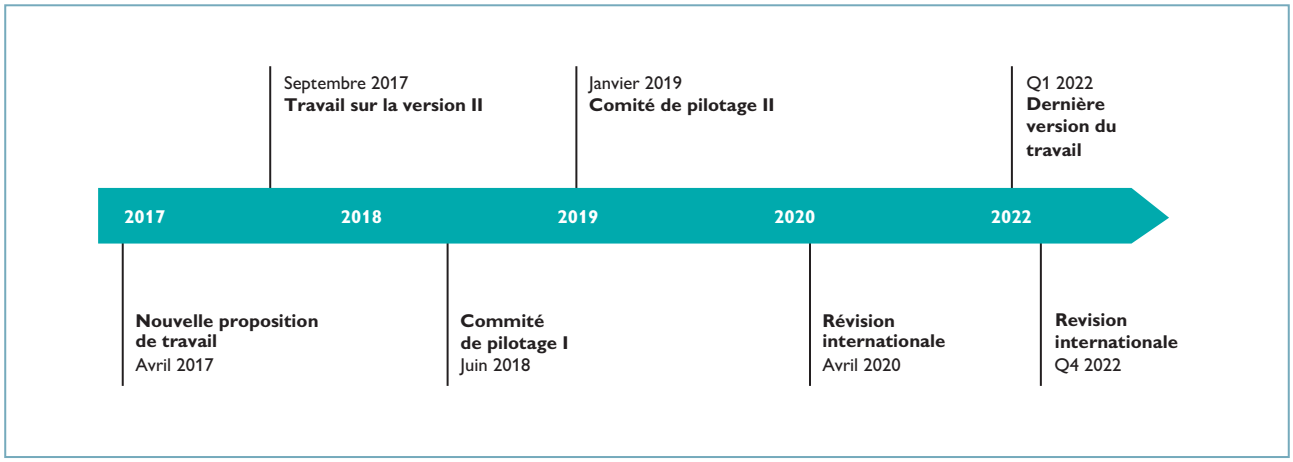
À quoi ressemble le travail d'un comité de normalisation ?

Avant de lancer un nouveau projet de normalisation au niveau international, il faut d'abord élaborer une proposition (NWIP = New Work Item Proposal) presque comme une « fiche signalétique ». Si ce processus est positif, le projet commence par la mise en place d'un groupe d'experts internationaux. C'est au sein de ce comité international que se déroulent les véritables travaux d'élaboration du contenu. Des projets de normes, appelés « commitee drafts » ou « FDIS », sont ensuite élaborés à partir du groupe de travail international. Ils sont ensuite mis à la disposition des organismes nationaux de normalisation, également appelés « comités miroirs », pour commentaires.
En Allemagne, le DIN prend souvent la tête des comités miroirs.

Expert en sécurité Carsten Gregorius de Phoenix Contact

Que se passe-t-il ensuite ?

En principe, chacun peut faire part de ses remarques ou de ses souhaits de modification d'un projet de norme par le biais des organismes nationaux de normalisation. C'est pourquoi, selon le projet de normalisation et le pays membre, il n'est pas rare que les commentaires comprennent des centaines de commentaires individuels qui doivent tous être traités. Mais comme les PME n'ont souvent pas le temps de participer aux différents comités de normalisation, des associations d'intérêt comme VDMA ou ZVEI prennent en charge une



Calendrier pour la révision de la norme EN ISO 13849

partie de ces tâches.

Et comment naît alors une nouvelle version d'une norme ?

Une fois que tous les commentaires des comités nationaux auront été renvoyés au groupe international de normalisation, ils seront pris en compte dans un nouveau projet. Celui-ci est ensuite mis à disposition sous forme de FDIS[8] pour le vote final des différents pays ayant le droit de vote. Un FDIS est alors adopté ou rejeté selon le principe de la majorité. En cas de résultat positif, la nouvelle version de la norme EN ISO 13849, par exemple, verra par la suite le jour.

Quels sont les prochains projets ?

Une fois la révision de la norme EN ISO 13849 (partie 1) terminée, le rapport technique EN ISO/TR 23849 sera complété par des modèles de calcul pour la détermination du PFH_D dans une prochaine étape de révision. Dans un autre projet, la partie 2 de la norme EN ISO 13849 (validation) sera révisée avant que les deux parties 1 et 2 ne soient ensuite fusionnées.

[8] FDIS : projet final de norme internationale

Glossaire

Couverture de diagnostic
Une mesure de l'efficacité du diagnostic, représentée en tant que rapport entre le taux de défaillance des taux d'erreur détectés et le taux de défaillances totales. La couverture de diagnostic peut soit se référer à l'ensemble du système, soit à certains composants tels que p. ex. pour les capteurs, les systèmes logiques ou les éléments finaux.

Défaillance dangereuse par heure
La probabilité d'une défaillance dangereuse par heure. PFHD signifie « Probability of dangerous Failure per Hour ».

Défaillance de cause commune
On entend par là la défaillance de fonctionnement de différents éléments provenant d'événements isolés communs.

Niveau de performance (Performance Level)

Le niveau de performance (PL) est une classification qualitative des différentes parties d'un système de commande relatives à la sécurité (composants de sécurité des systèmes de régulation et de commande) concernant la capacité de performance des différentes fonctions de sécurité en cas de situations imprévisibles.

Norme harmonisée
Les normes harmonisées sont des normes européennes pour les produits qui sont listés dans le Journal officiel sous une directive européenne. Elles appartiennent à la « New Approach » (nouveau concept) de la Commission européenne, visant à l'élaboration d'exigences fondamentales en matière de produits par les organisations CEN et CENELEC. Les normes harmonisées sont publiées dans le journal officiel de l'UE. Seules les marchandises et prestations de services conformes aux exigences fondamentales des directives peuvent être mises sur le marché. Elles sont identifiables

Contact

Réservez dès maintenant un rendez-vous conseils !

Vous cherchez un partenaire solide dans le domaine de la sécurité fonctionnelle ?

Fort de son expertise dans le domaine de la sécurité fonctionnelle, confirmée par sa certification TÜV Rheinland / FS Technician (#2100/2019), David est en charge de la gamme des produits safety chez Phoenix Contact France.

Il accompagne les clients dans leurs projets, apportant ses conseils sur des dossiers nécessitant une évaluation des risques jusqu'au choix des solutions à mettre en place afin d'atteindre le niveau de sécurité requis. N»hésitez pas à le contacter !

David Brynaert
Expert sécurité fonctionnelle
chez Phoenix Contact France

dbrynaert@phoenixcontact.fr

#FitForSafety

Littérature complémentaire et liens :

Sécurité fonctionnelle des machines – application pratique de la norme DIN EN ISO 13849-1
Édition Beuth : ISBN 978-3-410-25249-8

Safety meets Security – stratégie commune requise
Rendez-vous sur www.phoenixcontact.com/safety-meets-security

AI 04-22.002.L3