ZVEI:
Die Elektroindustrie

Sécurité des Machines

Guide d'interprétation et d'application des normes EN 62061 et EN ISO 13849-1

Edition II

Fachverband Automation

COLOPHON

Sécurité des Machines

Guide d'interprétation et d'application des normes EN 62061 et EN ISO 13849-1

Fédération Professionnelle de l'industrie
électronique et électrotechnique
Stresemannallee 19
60596 Frankfurt am Main
Allemagne
Association Professionnelle de l'Automatisation
Section des Systèmes de commutation, dispositifs
de commutation et contrôles industriels
Comité Technique Systèmes de Sécurité
dans l'Automatisation

Auteur: Dr. Markus Winzenick

Tél: +49 69 6302-426
Fax: +49 69 6302-319
Mail: winzenick@zvei.org
www.zvei.org/automation

Juin 2012

Sécurité des Machines

Vous êtes constructeur de machines, intégrateur de systèmes ou vous équipez des machines ?

Ce que vous devez prendre en compte au niveau de la sécurité fonctionnelle !

Explications pour l'application des normes EN 62061 et EN ISO 13849-1.

1. *Procédures de principe pour répondre aux exigences de la directive machine*

Que dois-je faire pour mettre sur le marché une machine conforme aux directives ?

La directive européenne exige qu'aucun danger ne doive émaner de la machine (évaluation du risque selon la norme EN ISO 12100). Étant donné que dans la technique le risque zéro n'existe pas, il s'agira d'atteindre un risque résiduel acceptable. Lorsque la sécurité dépend de systèmes de commande, ces derniers devront être construits de manière à ce que la probabilité de défauts fonctionnels soit réduite au minimum. Si cela n'est pas possible, les défauts apparaissant ne doivent alors pas conduire à une perte de la fonction de sécurité. Pour répondre à cette exigence, il est judicieux d'utiliser des normes harmonisées qui ont été élaborées selon un mandat de la Commission européenne et qui sont publiées dans le Journal officiel de l'Union européenne (effet de présomption). Ce n'est qu'ainsi qu'il est possible de prévenir un surcroît de coûts pour l'attestation de conformité.

Les deux normes EN 62061 et EN ISO 13849-1 seront comparées ci-après afin de faciliter les choix de l'utilisateur.

2. *Pourquoi la norme EN 954-1 n'est-elle désormais plus suffisante ?*

Jusqu'à présent, les parties des systèmes de commandes de machines relatives à la sécurité étaient conçues selon la norme EN 954-1. Dans cette norme, le risque évalué (catégorisé) servait de base. L'objectif était d'attribuer à chaque catégorie un comportement systématique en conséquence (approche déterministe). Mais, maintenant que l'électronique, et surtout l'électronique programmable, a fait son entrée dans la technique de sécurité, la sécurité ne peut plus être uniquement appréhendée avec le simple système de catégorisation de la norme EN 954-1. En outre, elle ne permet pas de se prononcer sur les probabilités de défauts (approches probabilistes).

Aussi bien la norme EN 62061 que la norme EN ISO 13849-1, qui succèdent à la norme EN 954-1, permettent désormais de remédier à la situation.

3. Domaines d'application (Scope) des deux normes

EN ISO 13849-1 : *« Parties des systèmes de commande relatives à la sécurité - Partie 1 : Principes généraux de conception »*

Cette norme peut être appliquée pour les SRP/CS (parties des systèmes de commande relatives à la sécurité et tout type de machine, quelles que soient les technologies et les énergies (électriques, hydrauliques, pneumatiques, mécaniques, etc.) utilisées).

La norme EN ISO 13849-1 énonce également des exigences spéciales pour les SRP/SC avec systèmes électroniques programmables.

EN 62061 : *« Sécurité fonctionnelle de systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité »*

Cette norme énonce des exigences et donne des recommandations pour la conception, l'intégration et la validation de systèmes de commande électriques, électroniques et électroniques programmables (SRECS) relatifs à la sécurité pour les machines.

Elle ne définit pas d'exigences pour la performance d'éléments de commande relatifs à la sécurité non électroniques (par ex. hydrauliques, pneumatiques ou électromécaniques) de machine.

4. Brève description de la norme EN ISO 13849-1

La norme EN ISO 13849-1 s'oriente sur les catégories connues de la norme EN 954-1:1996. Elle considère désormais également les fonctions de sécurité dans leur intégralité avec tous les appareils impliqués dans sa réalisation.

Au-delà de l'approche qualitative de la norme EN 954-1, la norme EN ISO 13849-1 apporte également une réflexion quantitative des fonctions de sécurité. Pour cela, des niveaux de performance (PL) seront utilisés en partant des catégories.

Suivant les types d'appareils, les caractéristiques relatives à la technique suivantes sont définies :

- Catégorie (exigence structurelle)
- PL : Niveau de performance
- $MTTF_d$: Durée moyenne jusqu'à une panne dangereuse (en: mean time to dangerous failure)
- B_{10d} : Nombre de cycles pour lesquels 10 % d'un échantillon des composants considérés comme soumis à l'usure ont eu une défaillance dangereuse.

- DC : Degré de couverture de diagnostic (en : diagnostic coverage)
- CCF : Défaillance due à une cause commune (en: common cause failure)
- T_M : Durée d'utilisation (en : Mission Time)

La norme décrit la recherche du niveau de performance (PL) pour les parties de systèmes de commande relatives à la sécurité sur la base d'architectures désignées (designated architectures) pour la durée d'utilisation prévue T_M.

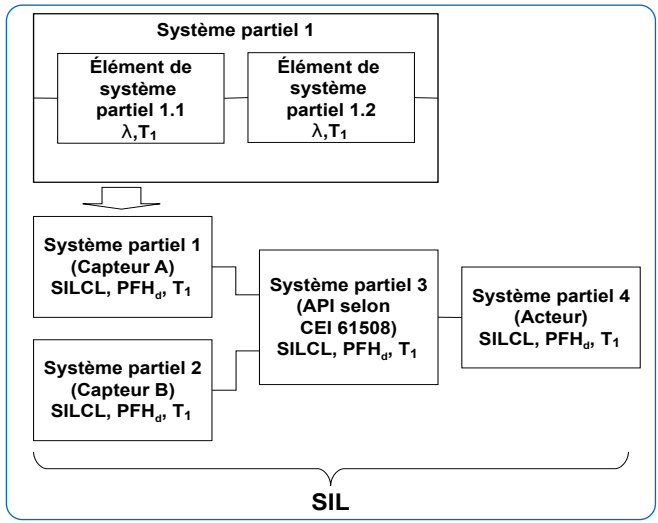
En cas de divergences à ce niveau, la norme EN ISO 13849-1 renvoie à la norme CEI 61508 pour les systèmes électriques/électroniques. La norme énonce des données pour la recherche du PL résultant pour un système complet composé à partir de plusieurs modules relatifs à la sécurité.

Pour la poursuite de la validation, la norme EN ISO 13849-1 renvoie à la partie 2 qui a déjà été publiée fin 2003. Cette partie énonce entre autres des données pour le traitement des défauts, la maintenance, la documentation technique ainsi que des consignes pour l'utilisation. La période de transition, pour passer de la norme EN 954-1 à la norme EN ISO 13849-1, au cours de laquelle les deux normes pouvaient être alternativement appliquées, a pris fin le 31 décembre 2011.

5. *Brève description de la norme EN 62061*

La norme EN 62061 est une norme spécifique au secteur issue de la norme CEI 61508. Elle décrit la réalisation de systèmes de commandes électriques et électroniques relatifs à la sécurité pour des machines et prend en considération l'ensemble du cycle de vie de la phase de conception à la mise hors service. Les approches quantitatives et qualitatives des fonctions de commande relatives à la sécurité en sont la base.

La capacité de performance d'une fonction de sécurité est énoncée par le **niveau d'intégrité de sécurité** (SIL). En partant ici des fonctions de sécurité révélées par l'analyse et l'évaluation du risque, on procédera à une répartition en fonctions de sécurité partielles puis à une assignation de ces fonctions de sécurités partielles à des appareils réels, appelés systèmes partiels et éléments de systèmes partiels. Sont traités aussi bien les matériels que les logiciels. Un système de commande relatif à la sécurité est composé de divers systèmes partiels. Les systèmes partiels sont décrits en matière de sécurité par les caractéristiques (aptitude SIL et PFH_d).



Caractéristiques en matière de sécurité pour les systèmes partiels :

- SILCL : Limite d'exigence SIL (aptitude, en: SIL claim limit)
- PFH_d : Probabilité de défaillance dangereuse par heure (en : probability of dangerous failure per hour)
- T_1 : La plus petite valeur à partir de la durée de vie attendue ou intervalle Proof-Test (en : life time or proof test interval)

Les systèmes partiels peuvent être eux-mêmes composés d'éléments de systèmes partiels (appareils) connectés de différentes manières présentant les caractéristiques pour déterminer la valeur PFH_d correspondante du système partiel.

Caractéristiques en matière de sécurité pour les éléments de systèmes partiels (appareils) :

- λ : Taux de défaillance (en : failure rate) ; pour les éléments soumis à l'usure (ou sans taux de défaillance constant) : valeur B_{10}
- SFF : Part de défaillances sûres (en : Safe Failure Fraction)

Pour les appareils électromécaniques, le taux de défaillance donné par le fabricant est indiqué par rapport à un nombre de cycles de commutations en tant que valeur B_{10}. Le taux de défaillance lié au temps et à la durée de vie attendue doit être déterminé au moyen de la fréquence de commutation pour chaque application.

Paramètres internes à déterminer lors de la conception/construction pour le système partiel qui sera composé d'éléments de systèmes partiels.

- T_2 : Intervalle de contrôle de diagnostic (en : diagnostic test interval)
- β : Réceptivité par rapport aux défaillances dues à une cause commune (en : susceptibility to common cause failure)
- DC : Degré de couverture de diagnostic (en : diagnostic coverage)

La valeur PFHd de la commande relative à la sécurité est déterminée en additionnant les valeurs PFH_d individuelles des systèmes partiels.

Lors de la réalisation d'une commande relative à la sécurité, l'utilisateur dispose des possibilités suivantes :

- Intégration d'appareils et de systèmes partiels qui répondent déjà à la norme EN ISO 13849-1 ou CEI 61508 ou EN 62061. La norme explique comment intégrer des appareils qualifiés lors de la réalisation de fonctions de sécurité.
- Développement de propres systèmes partiels.
  - Systèmes partiels électroniques, programmables ou systèmes partiels complexes : application de la norme CEI 61508.
  - Appareils simples et systèmes partiels : application de la norme EN 62061.

Cette norme énonce un système complet pour la réalisation de systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. La norme EN 62061 est harmonisée depuis décembre 2005.

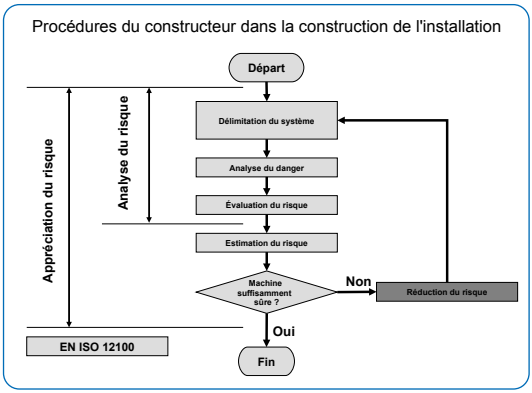
La norme EN ISO 13849-1 doit être utilisée pour les systèmes non électriques.

6. Étape par étape vers la sécurité – Procédures de principe

1ère étape – Évaluation du risque selon la norme EN ISO 12100

On part du principe qu'un danger inhérent à une machine entraînera tôt ou tard un dommage si aucune(s) mesure(s) de protection n'est(ne sont) adoptée(s). Les mesures de protection sont une combinaison des mesures effectuées par le constructeur et par l'utilisateur. Les mesures de protection qui ont été déjà prises lors de la phase de construction sont toujours à préférer aux mesures appliquées par l'utilisateur, elles se révèlent généralement plus efficaces que ces dernières.

En prenant en considération les expériences des utilisateurs de machines similaires et les échanges d'informations avec les utilisateurs potentiels (dans la mesure où cela est possible), le constructeur doit procéder dans l'ordre de prévalence suivant :



– détermination des limites et de l'utilisation conforme de la machine
– identification des dangers potentiels et des situations dangereuses inhérentes
– estimation du risque pour chaque danger et situation dangereuse identifiés
– évaluation du risque et prise de décisions sur la nécessité de réduction du risque

2e étape – Détermination des mesures pour réduire les risques estimés

L'objectif à atteindre est la réduction la plus importante possible du risque en prenant en compte différents facteurs. Le processus est itératif et, en utilisant au mieux les technologies disponibles, plusieurs répétitions consécutives peuvent être nécessaires pour réduire le risque.

Dans l'exécution de ce processus, il est nécessaire de prendre en compte l'ordre de prévalence suivant :

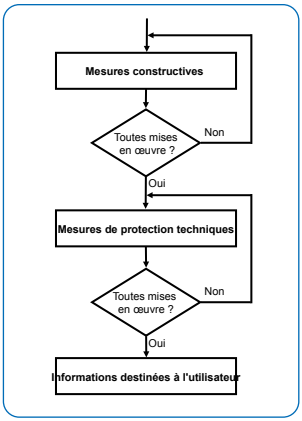
– la sécurité de la machine dans toutes les phases de sa durée de vie

– la capacité de la machine à effectuer sa fonction

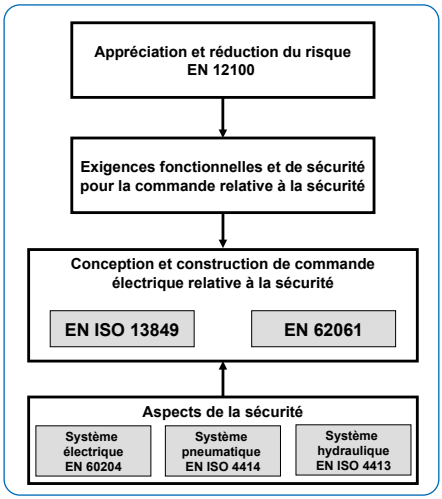
– l'utilisabilité de la machine

Ce n'est qu'une fois atteint ce niveau-là que les coûts de fabrication, d'exploitation et de démontage de la machine peuvent être pris en compte.

L'analyse du risque et le processus de réduction du risque exigent que les dangers soient éliminés ou réduits par des mesures de prévention hiérarchisées :



– suppression des dangers ou réduction du risque par des mesures constructives
– réduction du risque au moyen de dispositifs de sécurité et de mesures de protection complémentaires
– réduction du risque par la mise à disposition d'informations sur le risque résiduel destinées à l'utilisateur.



3e étape – Réduction du risque par des mesures de protection en matière de commande

Si la réduction du risque requise est réalisée au moyen de parties de commande relatives à la sécurité mettant en œuvre une mesure de protection, la conception de ces parties de commande est alors partie intégrante de la procédure de conception globale de la machine. Le système de commande relatif à la sécurité fournit la(les) fonction(s) de sécurité avec un SIL ou un PL qui réalise la réduction du risque requise.

4e étape – Réalisation en matière de commande en s'appuyant sur la norme EN 13849-1 ou EN 62061

1) Détermination de la performance requise

EN ISO 13849-1

Détermination du niveau de performance requis (PL_r)

S = Gravité de la blessure

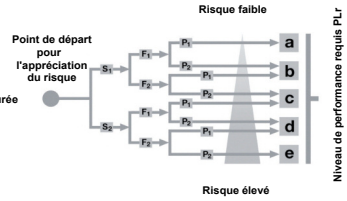
S1 = Blessure légère (normalement réversible)
S2 = Blessure grave, jusqu'à mortelle (généralement irréversible)

F = Fréquence et/ou durée d'exposition au danger

F1 = De rarement à peu fréquemment et/ou de courte durée
F2 = De souvent à permanente et/ou de longue durée

P = Possibilité d'éviter la mise en danger

P1 = Possible sous certaines conditions
P2 = Presque impossible



EN 62061

Évaluation du risque et détermination du niveau d'intégrité de sécurité (SIL)

Conséquence et gravité	S	Fréquence et durée	F	Probabilité de l'événement dangereux	W	Évitement	P	Classe K				
								3-4	5-7	8-10	11-13	14-15
Mort, perte d'un œil ou d'un bras	4	≤ 1/heure	5	Souvent	5			SIL2	SIL2	SIL2	SIL3	SIL3
Permanente, perte de doigts	3	> 1/heure - ≤1/jour	5	Probable	4				AM	SIL1	SIL2	SIL3
Réversible, traitement médical	2	> 1/jour - ≤2/semaines	4	Possible	3	Impossible	5			AM	SIL1	SIL2
Réversible, premiers soins	1	> 2/semaines - ≤1/an	3	Rarement	2	Possible	3				AM	SIL1
		> 1/an	2	Négligeable	1	Probable	1	AM = Autres mesures recommandées				

2) Spécification

La spécification des exigences fonctionnelles doit décrire les détails de chacune des fonctions de sécurité à réaliser. Pour cela, des interfaces nécessaires avec les autres fonctions de sécurité sont à définir et des réactions aux défauts nécessaires à déterminer. En outre, le SIL ou PL requis doit être déterminé.

3) Conception de l'architecture de commande

Un volet du processus de réduction du risque est la détermination des fonctions de sécurité de la machine. Ceci comprend les fonctions de sécurité de la commande, par ex. pour prévenir une mise en marche intempestive. Dans le processus de détermination des fonctions de sécurité, le fait qu'une machine a diverses modes opératoires (par ex. mode automatique, mode réglage) et que les mesures de protection peuvent être différentes selon ces modes opératoires (par ex. course lente en mode réglage <-> commande bimanuelle en mode automatique) doit toujours être pris en considération. Une fonction de sécurité peut être réalisée au moyen d'une ou plusieurs parties de commande relatives à la sécurité et plusieurs fonctions de sécurité peuvent se partager une ou plusieurs parties de commande relatives à la sécurité (par ex. modules de logique, élément(s) transmetteur d'énergie).

4) Détermination de la performance atteinte

EN ISO 13849-1

Une estimation du PL atteint doit être effectuée pour chaque SRP/CS sélectionné et/ou la combinaison de SRP/CS qui accomplit une fonction de sécurité.

Le PL du SRP/CS doit être déterminé par l'estimation des paramètres suivants :

- la valeur $MTTF_d$ ou B_{10d} des différents composants
- le DC
- la CCF
- la structure
- le comportement en cas de défaillance
- le logiciel relatif à la sécurité
- les défaillances systématiques
- la capacité à exécuter une fonction de sécurité dans des conditions ambiantes prévisibles
- l'application de principes de sécurité éprouvés

EN 62061

Le choix ou la conception du SRECS doit de principe répondre au minimum aux exigences suivantes :

- exigences pour l'intégrité de sécurité du matériel comprenant
- les limitations structurelles pour l'intégrité de sécurité du matériel
- les exigences pour la probabilité de pannes de matériel aléatoires représentant un danger

ainsi que les exigences pour l'intégrité de sécurité systématique comprenant

- les exigences pour la prévention de défaillances et
- les exigences pour la maîtrise de défaillance systématique.

La norme EN 62061 énonce également les exigences concernant la réalisation de programmes d'application.

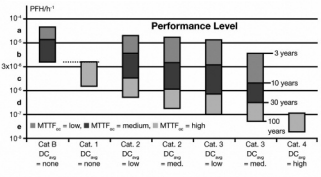
Caractéristiques en matière de sécurité pour les systèmes partiels :

- SILCL : Limite d'exigence SIL (aptitude, en: SIL claim limit)
- PFH_d : Probabilité de défaillance dangereuse par heure
- T_1 : Durée de vie attendue

EN ISO 13849-1

Niveau de performance (PL)	Probabilité moyenne d'une panne dangereuse [1/h]		
a	≥ 10-5	PFH_d	< 10-4
b	≥ 3x10-6	PFH_d	< 10-5
c	≥ 10-6	PFH_d	< 3x10-6
d	≥ 10-7	PFH_d	< 10-6
e	≥ 10-8	PFH_d	< 10-7

Rapport entre les catégories, la DC, le MTTFd et le PL



Remarque :
Les valeurs PFH représentent une condition indispensable pour la détermination du niveau de performance (PL). Par ailleurs, pour la détermination complète du PL on devra avoir recours à des mesures permettant de prévenir des défaillances telles que la CCF, catégorie ainsi que le DC.

EN IEC 62061

SIL (CEI 61508)	Probabilité moyenne d'une panne dangereuse [1/h]		
1	≥ 10-6	PFH_d	< 10-5
2	≥ 10-7	PFH_d	< 10-6
3	≥ 10-8	PFH_d	< 10-7

Paramètres en matière de sécurité pour les éléments de systèmes partiels (appareils) :

- λ: Taux de défaillance
- B_{10d} : Valeur pour les éléments soumis à l'usure (sans taux de défaillance constant)
- T_1 : Durée de vie attendue
- T_2 : Intervalle de contrôle de diagnostic
- β: Réceptivité par rapport aux défaillances dues à une cause commune
- DC : Degré de couverture de diagnostic
- SFF : Part de défaillances sûres (en : Safe failure Fraction)

SFF	HFT 0	HFT 1	HFT 2
< 60%	Non autorisé	SIL1	SIL2
de ≥ 60% à < 90%	SIL1	SIL2	SIL3
de ≥ 90% à < 99%	SIL2	SIL3	SIL3
≥ 99%	SIL3	SIL3	SIL3

EN ISO 13849-1	EN IEC 62061

Niveau de performance (PL)	SIL
a	-
b	1
c	
d	2
e	3

Remarque :
Le tableau décrit le rapport entre les deux concepts des normes (PL et SIL). Le « couplage PHF » servant de base dans ce tableau, n'est toutefois pas suffisant à lui seul pour l'évaluation.

5) Vérification

Le niveau de performance (PL) du(des) SRP/CS respectif(s) doit répondre au « niveau de performance requis » pour chacune des fonctions de sécurité. Les niveaux de performance de divers SRP/CS, qui sont parties d'une fonction de sécurité, doivent être supérieurs ou égaux au niveau de performance requis de cette fonction.

En cas d'interconnexion de plusieurs SRP/CS, le niveau de performance définitif peut être déterminé à l'aide du tableau 11 de la norme.

La probabilité d'une défaillance dangereuse de chaque SRCF comme conséquence de défaillances de matériel aléatoires dangereuses doit être égale ou inférieure à la valeur limite de défaillance déterminée dans la spécification des exigences de sécurité.

Le niveau d'intégrité de sécurité (SIL) qui, en raison des limitations structurelles, est atteint par le SRECS, est inférieur ou égal au SILCL minimum d'un système partiel quelconque impliqué dans l'exécution de la fonction de sécurité.

6) Validation

La conception d'une fonction de commande relative à la sécurité doit être validée. La pertinence de la fonction de commande relative à la sécurité pour l'application sera à vérifier. La validation peut se faire par analyse ou expertise (par ex. par simulation ciblée de défaillance individuelle ou multiple).

7. Glossaire

Abréviation	Terme anglais	Explication française
B_{10d}		Nombre de cycles, jusqu'à ce que 10 % des composants tombent en panne de manière dangereuse
λ	Failure Rate	Taux de défaillance
λ_s		Taux de défaillance pour des défauts non dangereux
λ_d		Taux de défaillance pour des défauts dangereux
CCF	Common Cause Failure	Défaillance due à une cause commune
DC	Diagnostic Coverage	Degré de couverture de diagnostic
DCavg	Average Diagnostic Coverage	Degré de couverture de diagnostic moyen
	Designated Architecture	Architecture désignée d'un SRP/CS
HFT	Hardware Fault Tolerance	Tolérance de défaut du matériel
MTBF	Mean Time Between Failures	Durée moyenne de défaillance qui s'écoule en service normal jusqu'à ce qu'une défaillance apparaisse.
MTTF	Mean Time To Failure	Durée moyenne jusqu'à une défaillance
$MTTF_d$	Mean Time To Dangerous Failure	Durée moyenne jusqu'à une défaillance dangereuse
MTTR	Mean Time To Repair	Durée moyenne de réparation (toujours nettement inférieure à la MTTF)
PFH	Probability Of Failure Per Hour	Probabilité d'une défaillance par heure
PFH_D	Probability Of Dangerous Failure Per Hour	Probabilité d'une défaillance dangereuse par heure
PL	Performance Level	Niveau de performance : Capacité de parties relatives à la sécurité d'exécuter une fonction de sécurité dans des conditions prévisibles pour répondre à la réduction du risque attendue.
PL_r	Performance Level required	Niveau de performance requis
SIL	Safety Integrity Level	Niveau d'intégrité de sécurité

Abréviation	Terme anglais	Explication française
SILCL	Safety Integrity Claim Limit	SIL Limite d'exigence (aptitude)
SRCF	Safety Related Control Function	Fonction de commande relative à la sécurité
SRP/CS	Safety Related Parts of a Control System	Partie relative à la sécurité d'un système de commande
SRECS	Safety Related Electrical Control Systems	Système de commande électrique relatif à la sécurité
T_1	Lifetime	Durée de vie du système de sécurité
T_2	Diagnostic Test Interval	Intervalle de contrôle de diagnostic
T_M	Mission Time	Durée d'utilisation
β	Susceptibility to Common Cause Failure	Réceptivité par rapport aux défaillances dues à une cause commune
C	Duty Cycle	Cycles d'actionnement (par heure) d'un module électromécanique
SFF	Safe Failure Fraction	Proportion de défaillances non dangereuses (sûres)
Security		Terme usuel pour désigner des services de sécurité ou de surveillance. Une personne ou une chose est protégée par surveillance.
Safety		Terme générique pour désigner entre autres la sécurité fonctionnelle et la sécurité des machines
Maschinen-sicherheit		Minimisation du risque atteinte à un risque résiduel acceptable grâce à l'adoption de mesures ressortant d'une analyse des dangers préalable
Funktionale Sicherheit		Partie de l'ensemble de la sécurité relatif à la machine et au système de commande de la machine, qui, pour réduire le risque, dépend du fonctionnement correct du SRECS, des systèmes relatifs à la sécurité de technologies autres et des dispositifs externes.

8. FAQ

Q : Existe t-il une énoncée SIL ou PL pour les vannes magnétiques / vannes ?

R : Non. Une énoncée SIL ou PL ne peut pas être donnée pour un composant individuel.

Q : Quelle est la différence entre SIL et SILCL ?

R : L'énoncée d'un SIL se rapporte toujours à une fonction de sécurité complète alors que le SILCL se rapporte à un système partiel.

Q : Y a-t-il une correspondance entre PL et SIL ?

R : Un rapport entre PL et SIL peut être déterminé au moyen de la valeur PFH_d. (cf. Étape 4 : « Détermination de la performance atteinte ») À noter : le tableau ne prend pas en considération les pré-requis spécifiques des deux normes en ce qui concerne la structure autorisée, le degré de couverture de diagnostic ou leurs exigences systématiques.

Probabilité moyenne d'une panne dangereuse [1/h]			Niveau de performance (PL) EN ISO 13849-1	Niveau SIL (CEI 61508)
≥ 10-5	PFH_d	< 10-4	a	-
≥ 3x10-6	PFH_d	< 10-5	b	1
≥ 10-6	PFH_d	< 3x10-6	c	
≥ 10-7	PFH_d	< 10-6	d	2
≥ 10-8	PFH_d	< 10-7	e	3

Q : À quel degré de couverture de diagnostic puis-je avoir recours pour les relais et vannes à contacts à guidage forcé ?

R : Conformément aux deux normes, un DC de 99 % peut être adopté pour les contacts à guidage forcé pour des vannes et des relais (à 2 canaux) installés de manière redondante.

La condition pré-requise étant ici une réaction au défaut adéquate ou au minimum un avertissement avant le danger.

Q : Puis-je atteindre la tolérance de défaut de matériel 1 avec un seul commutateur de porte de protection mécanique ?

R : Non, en règle générale, un défaut conduit déjà à une défaillance. Pour les systèmes à action magnétique ou basés sur la technologie RFID, le constructeur peut confirmer une tolérance de défaut de matériel de 1.

Q : Y a t-il une valeur PFHd pour les composants soumis à l'usure ?

R : Non, l'utilisateur peut déterminer une valeur PFHd pour les composants soumis à l'usure pour le cas d'application donné au moyen de la valeur B_{10} en dépendance du nombre de cycles d'actionnements.

Q : Quelle est la différence entre MTBF et MTTF ?

R : La MTBF décrit le temps écoulé entre 2 défauts, à l'inverse de la MTTF, durée jusqu'à ce qu'un défaut apparaisse.

Q : Que signifie « d » dans $MTTF_d$?

R : « d » représente « dangereux » à $MTTF_d$ décrit la durée jusqu'au premier défaut dangereux

Q : Puis-je appliquer la norme EN ISO 13849-1 pour l'intégration d'électronique complexe programmable ?

R : Oui. Toutefois, les exigences de la norme IEC 61508-3 devront être prises en considération pour le logiciel d'exploitation et les fonctions de sécurité selon PL « e ».

Q : Que puis-je faire si le fabricant de mes composants ne m'en délivre pas les caractéristiques ?

R : Les normes EN ISO 13849-1 et EN 62061 proposent en annexe des valeurs de références de remplacement pour des composants souvent utilisés. Il est toutefois toujours préférable d'utiliser les données originales du fabricant.

Q : Puis-je appliquer la norme EN ISO 13849-1 pour le calcul de la MTTF pour des vannes/armatures de process qui seront commutées moins d'une fois par an (Low Demand) ?

R : Non, la norme EN ISO 13849-1 ne décrit que le mode High Demand. C'est pourquoi une évaluation MTTF ne peut être faite qu'avec des mesures supplémentaires, telle que « dynamisation forcée ».

Q : Puis-je appliquer la norme EN 62061 pour le calcul du taux de défaillance pour des vannes/armatures de process qui seront commutées moins d'une fois par an (Low Demand) ?

R : voir question/réponse précédente

Q : Les logiciels d'application doivent-ils être certifiés ? Si « Oui » selon quelle norme ?

R : Non. Une obligation de certification sur la base des deux normes séparément pour les logiciels n'existe pas mais s'oriente sur le volume et la complexité du projet tout entier. Il est possible que dans le cadre de la vérification et de la validation de fonctions de sécurité, une vérification de logiciel soit nécessaire. Des informations à ce sujet se trouvent dans la norme EN ISO 13849-1 chapitre 4.6 et EN 62061 chapitres 6.9 et 6.10 ainsi que dans la norme EN 61508-3.

Q : Peut-on utiliser chaque composant avec MTTF pour la technique de sécurité ?

R : Non, en plus des caractéristiques statistiques telles que MTTF et B_{10}, le composant doit être également fonctionnel pour la fonction et répondre à certaines exigences minimales telles que les exigences constructives et se rapportant à la sécurité (mise place et application des principes de sécurité).

Fédération Professionnelle de l'industrie
électronique et électrotechnique
Lyoner Straße 9
60528 Frankfurt am Main
Allemagne

Association Professionnelle de l'Automatisation

Section des systèmes de commutation, dispositifs
de commutation et contrôles industriels

Comité Technique Systèmes de sécurité
dans l'automatisation